Unter www.philips.com/welcome können Sie Ihr Produkt registrieren und Unterstützung erhalten

CGA5722

DE WLAN ADSL Modem Router

PHILIPS

Inhaltsverzeichnis

1 Wichtig 2

1.1 Sicherheitsinformation 2

1.2 Informationen zur Netzwerkreichweite und Geschwindigkeit 2

1.3 Konformität 2

1.4 Recycling und Entsorgung 2

1.5 FCC-Erklärung bezüglich der Funkstrahlenbelastung 2

1.6 Softwarelizenzen 2

1.7 Haftungsausschluss 3

2 Ihr WLAN ADSL Modem Router 4

2.1 Verpackungsinhalt 4

2.2 Was Sie sonst noch benötigen 4

2.3 Vorderansicht des WLAN ADSL Modem Routers 5

2.4 Rückansicht des WLAN ADSL Modem Routers 5

3 Inbetriebnahme 6

3.1 Installieren 6

3.2 Anschließen 6

3.3 WiFi-Gerät installieren 7

3.3.1 WLAN USB Adapter SNU 5600 installieren 7

3.3.2 Ein anderes WiFi-Gerät installieren 7

4 WLAN Modem Router konfigurieren 8

4.1 Einloggen in die Webseiten 8

4.2 Menüstruktur der Web-Konfigurationsseiten 8

4.3 Web-Konfigurationsseiten ADSL / Internet 9

4.3.1 ADSL-Status/ADSL status 9

4.3.2 IP-Einstellungen/ISP settings 9

4.3.3 Parameter/Parameters 9

4.3.4 DNS 9

4.4 Web-Seiten für die Sicherheit 9

4.4.1 Firewall 9

4.4.2 WLAN Sicherheit/Wireless Security 12

4.5 Webseiten zur Einstellung von Heimnetzwerken 13

4.5.1 Status 13

4.5.2 Netzwerk-Einstellungen/Network settings 13

4.5.3 Drahtlos (WLAN)/Wireless 13

4.6 Webseiten für erweiterte Einstellungen/ Advanced settings webpages 14

4.6.1 NAT 14

4.6.2 Instandhaltung/Maintenance 15

4.6.3 System 16

4.6.4 SNMP 17

4.7 UPNP 17

4.8 QoS 18

4.9 DDNS 18

4.10 Routing 18

4.11 INSTALLATIONS-ASSISTENT/SET UP WIZARD 19

5 Technische Daten 21

6 Häufig gestellte Fragen 23

1 Wichtig

Nehmen Sie sich vor der Benutzung des WLAN ADSL Modem Routers etwas Zeit, um die Bedienungsanleitung durchzulesen. Sie enthält wichtige Informationen und Hinweise für die Bedienung Ihres neuen WLAN ADSL Modem Router.

1.1 Sicherheitsinformation

Achtung

- Verwenden Sie nur den mitgelieferten Netzadapter für die Stromversorgung dieser Geräteausstattung.
- Für die Stromversorgung nur den Netzadapter "Leader: MU12-2120100-C5" und/oder "Jentec: AH1212-E" benutzen!
- Verwenden Sie nur die mitgelieferten Anschlusskabel.
- Die Funkausstattung für WLAN-Anwendungen ist nicht vor Beeinträchtigungen durch andere Funkdienste geschützt.
- Das Gerät darf nicht Feuchtigkeit, Regen, Sand oder starker Hitze ausgesetzt werden.
- Das Gerät vor Wasserspritzer und Staub schützen.
- Stellen Sie keine mit Flüssigkeiten gefüllten Gegenstände, z.B. Vasen, auf das Gerät.
- Setzen Sie das Gerät nicht extrem hohen Temperaturen aus, z.B. in der Nähe von Heizgeräten oder an Orten mit direkter Sonneneinstrahlung.
- Sorgen Sie für einen ausreichenden Abstand zwischen dem Gerät und anderen Gegenständen, um die Belüftung nicht zu beeinträchtigen.
- Öffnen Sie das Gerät nicht. Setzen Sie sich mit Ihrem IP / Kabel-provider in Verbindung.

1.2 Informationen zur Netzwerkreichweite und Geschwindigkeit

- Umgebung: Funksignale können Gebäudegrenzen überwinden, insbesondere wenn die drahtlosen Komponenten in direkter Reihe und in Sichtweite angeordnet sind. Das Aufstellen der drahtlosen Komponenten an höhergelegenen Positionen verhindert physikalische Beeinträchtigungen und gewährleistet eine bessere Reichweite.
- Bauliche Hindernisse wie Metallrahmen und Stahlbeton sowie Hausmauern und Fußböden beeinträchtigen die Stärke der Funksignale. Vermeiden Sie drahtlose Komponenten in unmittelbarer Nähe von großen, massiven oder metallhaltigen Gegenständen aufzustellen, wie z.B. Computer, Bildschirme oder ähnliche Geräte.
- Reichweite, Geschwindigkeit und Stärke der drahtlosen Signale können durch benachbarte, drahtlose Netzwerke und Geräte beeinflusst werden. Elektromagnetische Geräte wie Fernseher, Radios, Mikrowellenherde und schnurlose Telefone, speziell im Frequenzbereich 2,4 GHz, können die drahtlose Übertragung ebenfalls beeinträchtigen.
- Wenn Personen in unmittelbarer Nähe der WLAN-Geräteausstattung stehen oder sitzen, kann die Funksignalqualität eingeschränkt werden.
- Ausrichten der Antenne: Antennen niemals in unmittelbarer Nähe von großen Metallgegenständen aufstellen, dies kann Störungen verursachen.

1.3 Konformität

Hiermit erklärt Philips die Übereinstimmung des Gerätes mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG.
Die Konformitätserklärung finden Sie unter www.p4c.philips.com.

Gemäß dieser Richtlinie kann das Produkt in folgenden Ländern eingesetzt werden:

B	✓	DK	✓	E	✓	GR	✓	F	✓
IRL	✓	I	✓	L	✓	NL	✓	A	✓
P	✓	SU	✓	S	✓	UK	✓	N	✓
D	✓	CH	✓	TR	✓				

1.4 Recycling und Entsorgung

Anweisungen für die Entsorgung alter Produkte:
Die Richtlinie WEEE (Abfall aus elektrischen und elektronischen Geräteausstattungen; 2002/96/EG) wurde zum Schutz der menschlichen Gesundheit und der Umwelt aufgestellt, um sicherzustellen, dass ausgediente Produkte unter Nutzung der bestmöglichen Wiederaufbereitungs-, Rückgewinnungs- und technischen Recycling-Möglichkeiten entsorgt werden.
Ihr Produkt wurde aus hochwertigen Materialien und Komponenten entwickelt und hergestellt, die wiederaufbereitet und weiterverwendet werden können.

Werfen Sie Ihr altes Produkt nicht in den Hausmüll.
Bitte informieren Sie sich über die örtlichen Sammelstellen für elektrische und elektronische Abfallprodukte, die mit diesem Symbol gekennzeichnet sind:

Nutzen Sie bitte eine der nachfolgenden Entsorgungsmöglichkeiten:

- Entsorgen Sie das komplette Produkt (einschließlich der Kabel, Stecker und des Zubehörs) bei der zuständigen WEEE-Sammelstelle.
- Wenn Sie ein Ersatzprodukt erwerben, können Sie Ihr Altgerät im Fachgeschäft abgeben. Gemäß der Richtlinie WEEE ist der Einzelhandel verpflichtet, Altgeräte zurückzunehmen.

Empfehlungen für die Entsorgung des Verpackungsmaterials:
Philips hat die Geräteverpackungen mit Standardsymbolen gekennzeichnet, um die ordnungsgemäße Entsorgung zu fördern.
Es wurde ein finanzieller Beitrag an die nationalen Institutionen für Wiederaufbereitung und Recycling geleistet.
Das gekennzeichnete Verpackungsmaterial kann dem Recycling zugeführt werden.

1.5 FCC-Erklärung bezüglich der Funkstrahlenbelastung

Diese Geräteausstattung entspricht der FCC-Strahlenbelastungsgrenze für eine nicht überwachte Umgebung. Beim Aufstellen und Betrieb des Gerätes ist ein Mindestabstand von 20 cm zwischen dem Funkgerät und Ihrem Körper einzuhalten.

1.6 Softwarelizenzen

Dieses Produkt enthält frei zugängliche Softwarepakete (Open Source Software Packages). Eine Übersicht der Softwarepakete, die Lizenzen und / oder diesbezügliche Anmerkungen sowie die Referenz-Codes für einige dieser Pakete finden Sie in der Online-Produktdokumentation, die unter www.p4c.philips.com aufgerufen werden kann.

1.7 Haftungsausschluss

Dieses Produkt wird von “Philips” “ohne Mängelgewähr” sowie ohne ausdrückliche oder implizite Garantie bereitgestellt, inklusive der, jedoch nicht beschränkt auf die, implizite(n) Zusicherung der allgemeinen Gebrauchstauglichkeit für einen bestimmungsgemäßen Einsatz.

Philips ist unter keinen Umständen für direkte, indirekte, zufällige, besondere, beispielhafte oder Folgeschäden haftbar zu machen (inklusive, jedoch nicht beschränkt auf, der / die Geltendmachung von Ersatzgütern und -dienstleistungen, Verlust von Informationen, Daten oder Umsätzen, sowie Geschäfts- und Betriebsunterbrechungen), wie auch immer verursacht und unter jeglicher Haftungstheorie, ob als Vertrags-, Kausal- oder Schadenshaftung (inklusive Fahrlässigkeit oder Ähnlichem) entstehend aus jedweder Unfähigkeit zur Nutzung dieses Produktes, auch im Fall der vorherigen Inbetrachtziehung der Möglichkeit solcher Schäden.

Desweiteren übernimmt Philips keine Garantie für die Fehlerfreiheit und Vollständigkeit der Informationen, Texte, Grafiken, Links sowie sämtlicher anderer von diesem Produkt übertragenen Elemente.

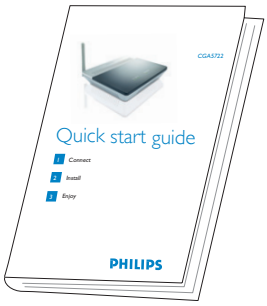
2 Ihr WLAN ADSL Modem Router

Herzlichen Glückwunsch zu Ihrem Kauf und willkommen bei Philips!

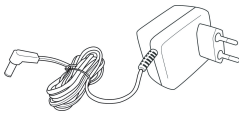
Um den Support von Philips optimal zu nutzen, registrieren Sie Ihr Produkt bitte unter: www.philips.com/welcome.

2.1 Verpackungsinhalt

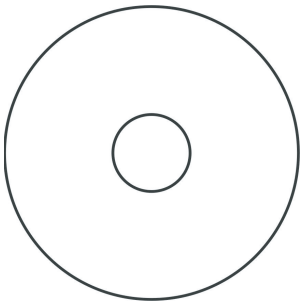
WLAN ADSL Modem Router



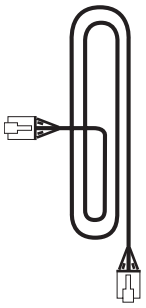
Kurzbedienungs-anleitung



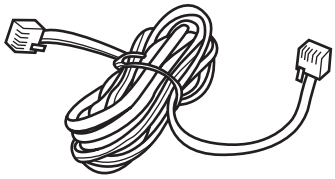
Netzadapter



Installations-CD-ROM



Ethernet-Kabel (RJ-45)



Telefonkabel (RJ-11)

2.2 Was Sie sonst noch benötigen

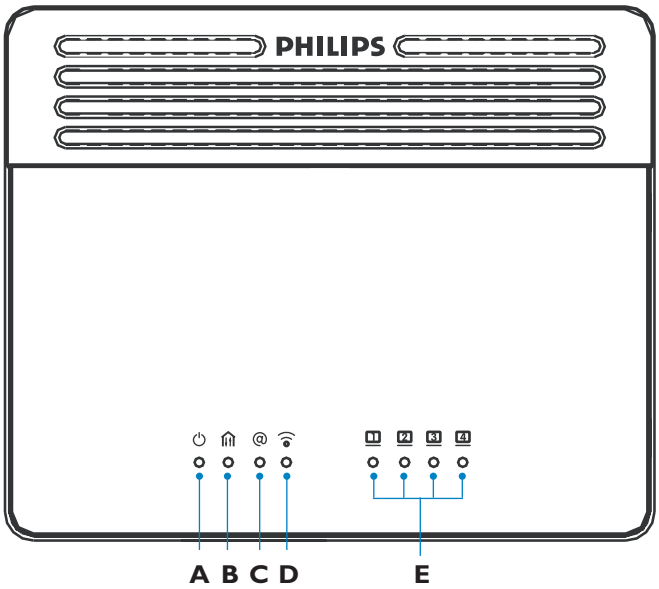
Einen ADSL-Filter, der an Ihren Telefonstecker angepasst ist

Einen PC oder Laptop mit einem freiem USB-Port

Einen Internet-Browser

Einen Internet-Anschluss

2.3 Vorderansicht des WLAN ADSL Modem Routers



A
EIN: Stromversorgung eingeschaltet, normaler Betrieb
AUS: Stromversorgung ausgeschaltet oder Funktionsfehler

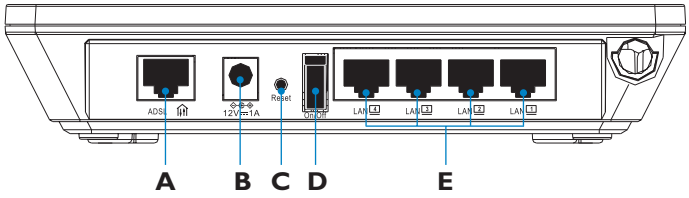
B
EIN: die ADSL-Verbindung ist aufgebaut
Blinkt: Startvorgang
AUS: keine ADSL-Verbindung

C
EIN: die Internet-Verbindung ist aufgebaut
AUS: keine Datenübertragung

D
EIN: die drahtlose Funkverbindung ist aufgebaut
Blinkt: Senden / Empfang von Daten
AUS: keine Datenübertragung

E
EIN: die Ethernet-Verbindung ist aufgebaut
Blinkt: Senden / Empfang von Daten
AUS: keine Verbindung

2.4 Rückansicht des WLAN ADSL Modem Routers



A ADSL-Port
ADSL-Port (RJ-11). Schließen Sie das mitgelieferte Telefonkabel an diesem ADSL-Port an.

B Stromversorgungsbuchse
Schließen Sie den mitgelieferten Netzadapter an dieser Buchse an.

Achtung
Wenn Sie einen falschen Netzadpater anschließen, kann die ADSL WLAN Basisstation beschädigt werden.

C Reset-Knopf
Verwenden Sie diesen Knopf, wenn Sie die Stromversorgung und die Werkseinstellungen zurücksetzen möchten. Zum Zurücksetzen ohne Verlust der Konfigurationseinstellungen, siehe 4.6.2.

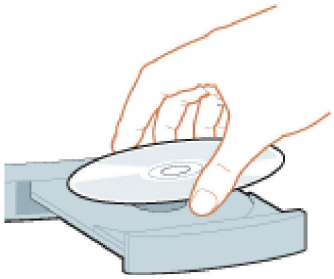
D EIN- / AUSschalter
Ein- / Ausschalter, um das Gerät EIN- / AUSzuschalten.

E LAN-Ports
Ethernet-Ports 10/100 (RJ-45). Verwenden Sie diese Ports, um die Geräte an Ihrem lokalen Netz anzuschließen (z.B., ein PC, Hub, oder Switch).

3 Inbetriebnahme

3.1 Installieren

1 Legen Sie die Installations-CD in das CD-ROM- (oder DVD-ROM-) Laufwerk Ihres PC's ein



- *Das Installationsprogramm startet automatisch*

2 Befolgen Sie die Anweisungen auf dem Bildschirm

Hinweis

Sollte die Installation nicht automatisch starten:

1 Klicken Sie unter Windows auf **START** und dann auf **AUSFÜHREN**
2 Geben Sie **explorer** ein und wählen Sie Ihr CD-ROM- (oder DVD-ROM-) Laufwerk aus
3 Doppelklicken Sie auf **Setup.exe**

Tipp

Standardmäßig wird die Sprache Ihres Betriebssystems eingestellt. Sie haben 10 Sekunden, um eine andere Sprache auszuwählen.

3 Klicken Sie auf die gewünschte Sprache

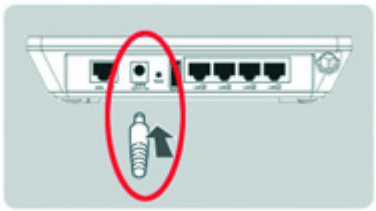
- *Das nächste Fenster erscheint automatisch*

4 Klicken Sie auf die Abbildung des WLAN Modem Routers CGA5722

- *Das nächste Fenster erscheint automatisch*

3.2 Anschließen

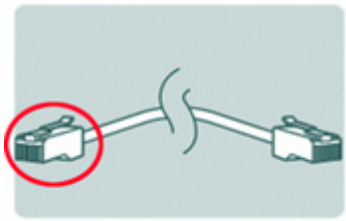
1 Schließen Sie den mitgelieferten Netzadapter am 12V ===1A Port an und schalten Sie EIN



2 Stecken Sie das andere Ende des Netzkabels in eine Stromversorgungsdose

- *Die Stromversorgungsanzeige leuchtet*

3 Nehmen Sie das mitgelieferte Ethernet-Kabel aus der Verpackung

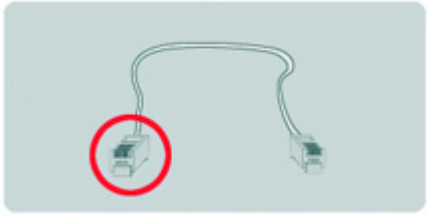


4 Schließen Sie dieses Ethernet-Kabel am LAN 1 Port des CGA5722 an

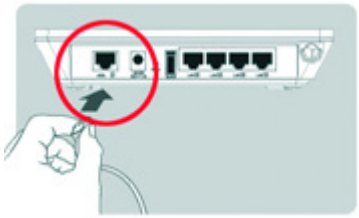
5 Schließen Sie das andere Ende des Ethernet-Kabels an Ihrem Computer an

- *Die LAN 1-Anzeige leuchtet*

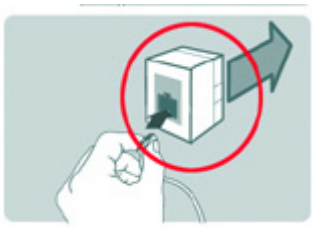
6 Nehmen Sie das mitgelieferte Telefonkabel aus der Verpackung



7 Schließen Sie das mitgelieferte Telefonkabel am ADSL-Port an



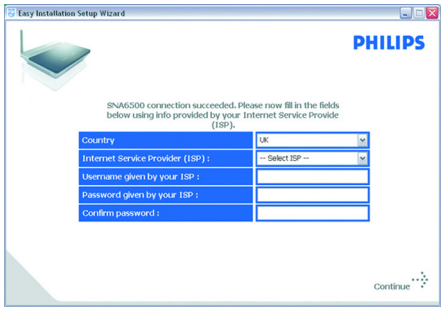
8 Schließen Sie das andere Ende des mitgelieferten Telefonkabels am ADSL-Filter an und stecken Sie dann den ADSL-Filter in eine Telefondose



- *Die Anzeige leuchtet*

9 Klicken Sie dann auf **Weiter**
- *Ein Fortschrittsbalken erscheint*

10 Wählen Sie Ihr Land und Ihren Internet-Provider (IP) aus; diese Angaben finden Sie in den Unterlagen von Ihrem IP


Easy Installation Setup Wizard
PHILIPS
SNA6500 connection succeeded. Please now fill in the fields below using info provided by your Internet Service Provide (ISP).
Country
UK
Internet Service Provider (ISP) :
-- Select ISP --
Username given by your ISP :
Password given by your ISP :
Confirm password :
Continue

Hinweis

Wenn Ihr IP nicht in der Standardliste enthalten ist, wählen Sie "**Andere**".

11 Klicken Sie auf **Weiter**
- *Ein Balken informiert Sie über den Fortschritt der Installation, Ihre Parameter werden gespeichert und es wird eine Verbindung zum Internet hergestellt*
- *Sobald die Installation abgeschlossen ist, erscheint nebenstehendes Fenster*

Hinweis

Dieses Fenster ist die Philips Support Site. Es ist die Original-Internet-Seite, Änderungen vorbehalten. Das auf Ihrem PC angezeigte Fenster kann sich von dem hier abgebildeten Fenster unterscheiden.

12 Klicken Sie auf **Menü** für die Rückkehr zum Menü-Fenster

Tipp

Ihr WiFi-Netzwerk ist betriebsbereit, aber noch nicht geschützt.

13 Klicken Sie auf **Verschlüsselung einstellen**

- *Ihr WiFi-Netzwerk wird jetzt automatisch abgesichert*
- *Sie können weder das Verschlüsselungswort noch den Netzwerknamen (SSID) auswählen*

Hinweis

Sie können die WLAN-Schutzeinstellungen jederzeit abrufen, indem Sie die Intallations-CD-ROM auf dem gleichen Computer verwenden, auf dem Sie den Modem Router installiert haben, und auf der Menüseite auf das Sicherheitsymbol klicken.

3.3 WiFi-Gerät installieren

Wenn Sie ein WiFi Gerät installieren möchten, müssen Sie Ihre WLAN-Schutzeinstellungen wiederverwenden, indem Sie die Installations-CD-ROM auf dem gleichen Computer einsetzen, auf dem Sie den Modem Router installiert haben, und auf der Menüseite auf das Sicherheitsymbol klicken.

3.3.1 WLAN USB Adapter SNU 5600 installieren

Wenn Sie das Starterkit CKA5720 gekauft haben, ist der WLAN USB Adapter SNU5600 Bestandteil des Verpackungsinhaltes. In diesem Fall brauchen Sie nur die Installations-CD-ROM, die mit dem CKA5720 mitgeliefert wurde, einzulegen und die Anweisungen auf dem Bildschirm zu befolgen.

3.3.2 Ein anderes WiFi-Gerät installieren

1 Lesen Sie die Bedienungsanleitung des WiFi-Gerätes

Hinweis

Wenn Sie Ihr Netzwerk bereits mit der "Einfachen Installation" gesichert haben (siehe Abschnitt 3.2, Bedienschritt 13), lautet die SSID "PHILIPS_xxxxxx".
Wenn das Netzwerk noch nicht mit der "Einfachen Installation" gesichert wurde, lautet die SSID "philips_install".
Falls Sie einen anderen Netzwerknamen verwendet haben, wird dieser Name angezeigt anstelle von "PHILIPS_xxxxxx" oder "philips_install".

Hinweis

Sie können die WLAN-Schutzeinstellungen jederzeit deaktivieren, indem Sie die Intallations-CD-ROM auf dem gleichen Computer verwenden, auf dem Sie den Modem Router installiert haben, und auf der Menüseite auf das Sicherheitsymbol klicken.

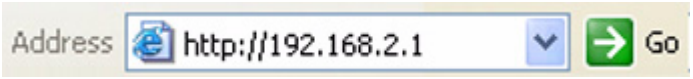
4 WLAN Modem Router konfigurieren

Fortgeschrittene Anwender möchten bei Bedarf die Konfiguration des WLAN Modem Routers ändern können. In diesem Kapitel finden Sie Informationen für den Zugriff auf die Web-Konfigurationsseiten, zur Struktur dieser Webseiten und Erläuterungen zu den einzelnen Seiten.

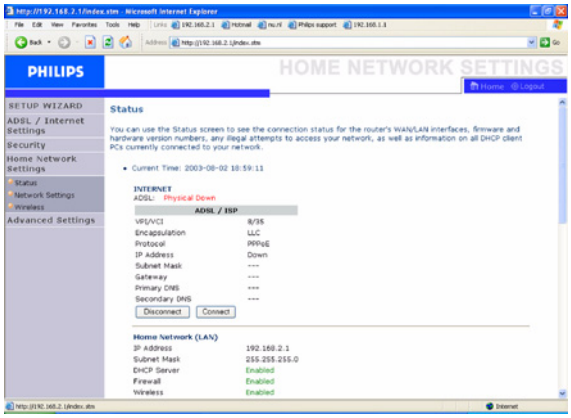
4.1 Einloggen in die Webseiten

1 Rufen Sie Ihren Internet-Browser auf

2 Geben Sie im Adressfeld *http://192.168.2.1* ein



3 Klicken Sie auf **GO**
- *Die nachfolgende Webseite wird angezeigt*



Hinweis
Die Standardsprache ist ausschließlich Englisch.

4 Um die gewünschte Webseite aufzurufen, klicken Sie auf das entsprechende Register, links auf der Seite

4.2 Menüstruktur der Web-Konfigurationsseiten

In der nachfolgenden Tabelle ist der Menübaum der Webseiten aufgelistet.

SET UP WIZARD	Getting started
	Wireless settings
	ADSL settings
	Confirm
	Connection status

Hinweis
Es wird dringend empfohlen anstelle des Installations-Assistenten (Set up Wizard) das auf der mitgelieferten CD-ROM bereitgestellte "Einfache Installationsprogramm" zu verwenden.

ADSL / Internet Settings	ADSL status
	ISP settings
	Parameters
	DNS

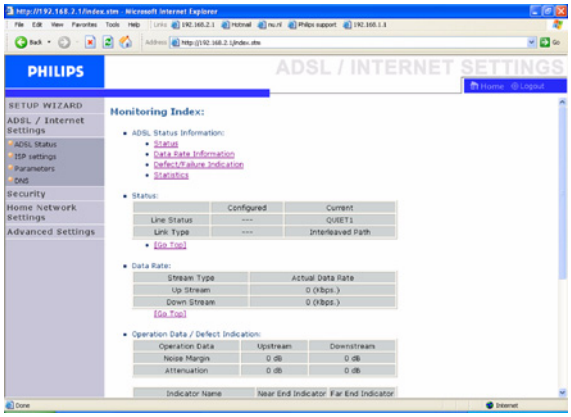
Security	Firewall
	Access Control
	MAC Filter
	URL blocking
	Schedule Rule
	Intrusion Detection
	DMZ
Wireless Security	
	Wireless Encryption
	Access control
	WEP
	WPA
	802.1X

Home Network Settings	Status
	Network settings
	Wireless
	Channel and SSID
	Access control
	WDS
	WEP
	WPA
	802.1X

Advanced settings	NAT
	Address Mapping
	Virtual Server
	Special Applications
	NAT Mapping Table
Maintenance	
	Configuration Tools
	Firmware Upgrade
	Reset
System	
	Time Settings
	Password Settings
	Remote Management
SNMP Community	
	SNMP Community
	SNMP Trap
UPNP	
QoS	
	Traffic mapping
	Traffic statistics
DDNS	
Routing	
	Static route
	RIP
	Routing table

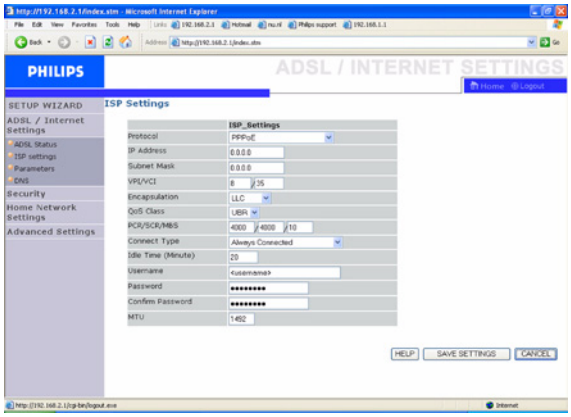
4.3 Web-Konfigurationsseiten ADSL / Internet

4.3.1 ADSL-Status/ADSL status



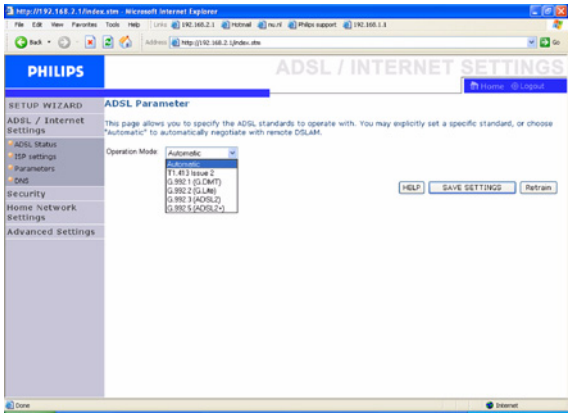
Klicken Sie auf “ADSL Status” auf der linken Seite des Bildschirmfensters. Das Hauptmenü wird links angezeigt und auf der rechten Seite erscheinen Informationsangaben.

4.3.2 IP-Einstellungen/ISP settings



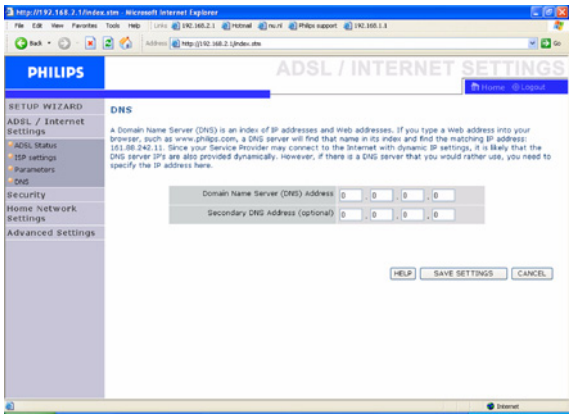
Geben Sie hier die IP-Parameter ein, die Sie von Ihrem Internet-Provider erhalten haben.

4.3.3 Parameter/Parameters



Auf dieser Seite können Sie die gewünschten ADSL-Funktionsstandards einstellen. Sie können entweder einen der angebotenen Standards einstellen oder “Automatic” auswählen für die Verbindung mit dem DSLAM.

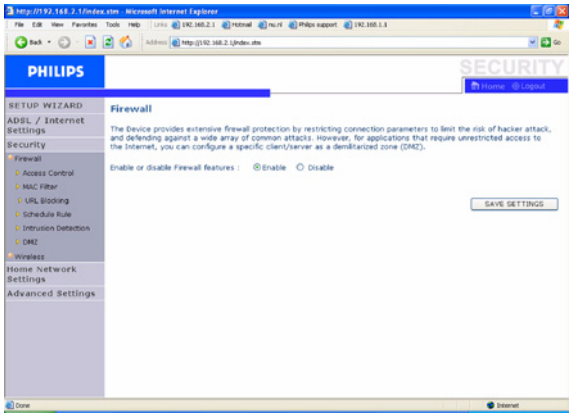
4.3.4 DNS



Die Server für Domänennamen (DNS) dienen der Zuordnung des Domänennamens (z.B. www.philips.com) und der IP-Adresse (z.B. 64.147.25.20). Im Regelfall wird die DNS-Adresse automatisch konfiguriert. Wenn dies nicht der Fall ist, erhalten Sie von Ihrem Internet-Provider eine oder mehrere DNS-Adressen.

4.4 Web-Seiten für die Sicherheit

4.4.1 Firewall



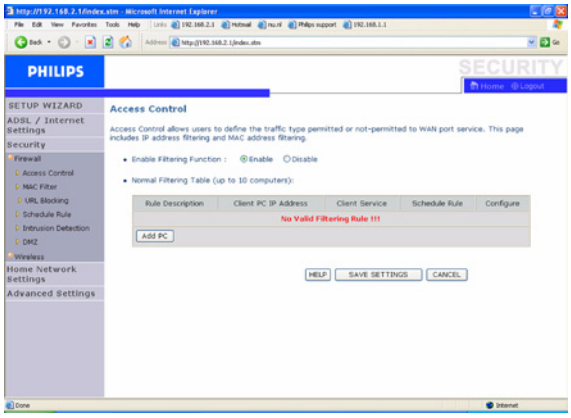
Die Firewall der ADSL-WLAN-Basisstation überprüft Pakete am Anwendungslayer, hält TCP- und UDP-Sitzungsinformationen auf Stand, inklusive Time-outs und der Anzahl der aktiven Sitzungen, und ist in der Lage, bestimmte externe Netzwerkangriffe zu entdecken und zu verhindern.

Netzwerkangriffe, die den Zugriff auf ein Netzwerkgerät verhindern, werden als Denial-of-Service (DoS) -Angriffe bezeichnet. DoS-Angriffe zielen auf Geräte und Netzwerke ab, die einen Zugang zum Internet haben. Es ist nicht deren Ziel, Informationen zu entwenden, sondern ein Gerät oder Netzwerk außer Betrieb zu setzen, damit der Benutzer keinen Zugang mehr zu den entsprechenden Netzwerkquellen hat.

Die Firewallfunktion der ADSL-WLAN-Basisstation schützt vor folgenden DoS-Angriffen: IP Spoofing, Land Attack, Ping of Death, IP Zero Length, Smurf Attack, UDP Port Loopback, Snork Attack, TCP Null Scan und TCP SYN Flooding.

Die Firewall beeinträchtigt die Systemleistung nur geringfügig, deswegen empfehlen wir, diese zum Schutz des Netzwerks aktiviert zu lassen. Wählen Sie “Enable” und klicken Sie auf die Schaltfläche “SAVE SETTINGS”, um die Firewall-Untermenüs zu öffnen.

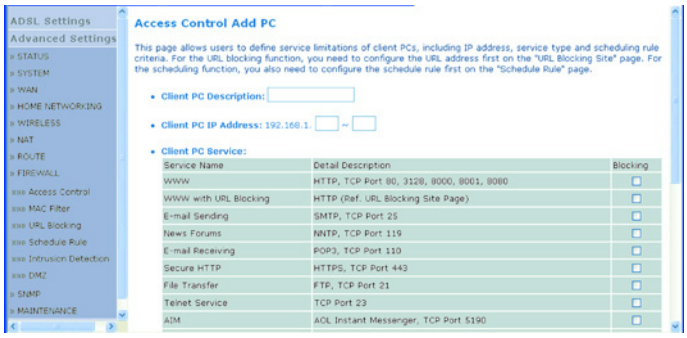
Zugangskontrolle/Access Control:



Die Zugangskontrolle ermöglicht den Benutzern den erlaubten oder nicht erlaubten abgehenden Datenverkehr über die WAN-Schnittstelle zu definieren. Standardmäßig ist der gesamte abgehende Datenverkehr zugelassen.

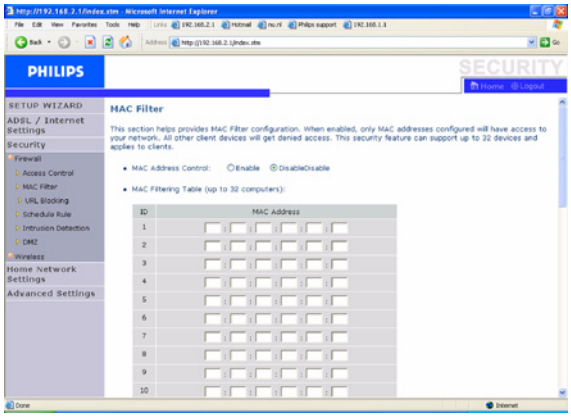
Um den PC in die Filterungs-Tabelle einzufügen:

1- Klicken Sie im Zugangskontroll-Fenster auf “Add PC”



2- Definieren Sie die entsprechenden Einstellungen für die PC-Client-Dienste
3- Klicken Sie auf “OK” und dann auf “SAVE SETTINGS”, um Ihre Einstellungen zu speichern

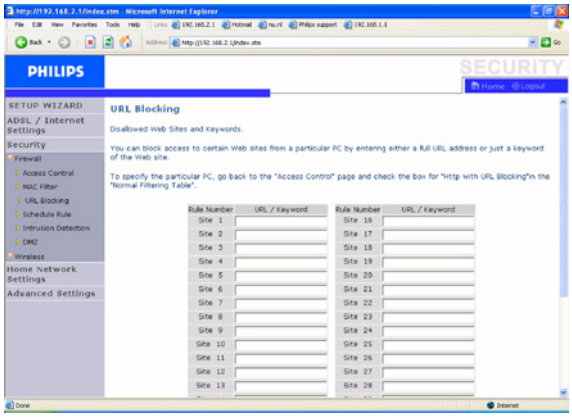
MAC-Filter/MAC filter:



Mit der ADSL-WLAN-Basisstation kann der Netzzugang auch über die MAC-Adressen eingeschränkt werden. In der Tabelle für die Filterung der MAC-Adressen können für die ADSL-WLAN-Basisstation bis zu 32 MAC-Adressen eingegeben werden, die berechtigt sind auf das WAN-Port zuzugreifen.

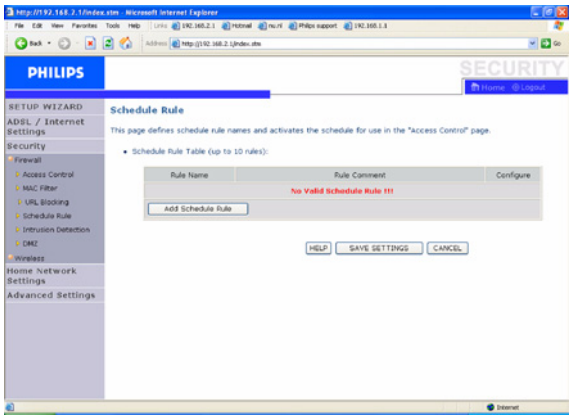
1- Klicken Sie auf “Yes”, um die Funktion zu aktivieren oder auf “No”, wenn Sie die Funktion deaktivieren möchten
2- Geben Sie die MAC-Adresse im vorgegebenen Feld ein und klicken Sie auf “Save Settings” zum Bestätigen

URL sperren/URL Blocking:



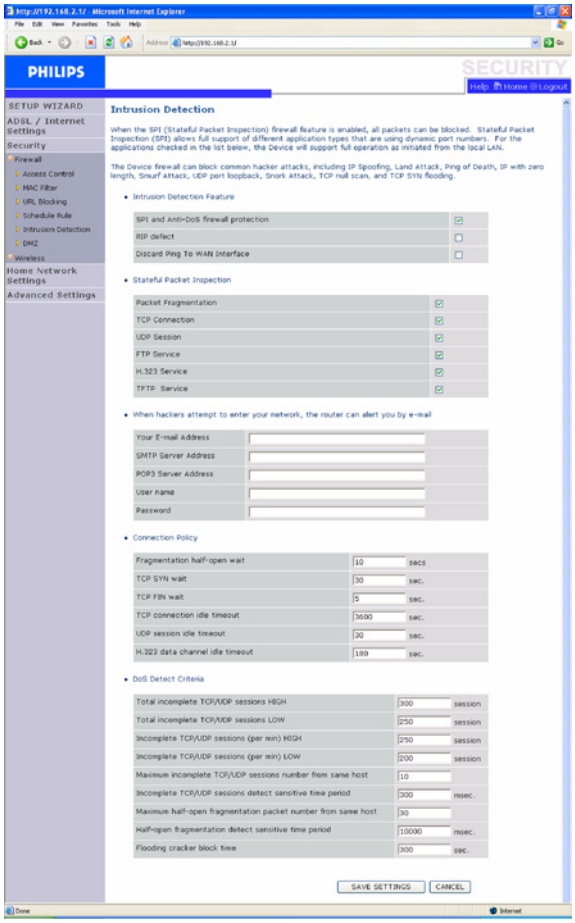
Mit der ADSL-WLAN-Basisstation kann der Benutzer den Zugriff auf bestimmte Web-Seiten sperren, indem entweder die komplette URL-Adresse oder nur ein Schlüsselwort eingegeben wird. Diese Funktion kann auch dazu benutzt werden, um Kindern den Zugang zu gewalttätigen oder pornographischen Web-Seiten nicht zu ermöglichen.

Zeitregeln/Schedule Rule:



Sie können den Internet-Zugang der lokalen Clients durch Regeln begrenzen. Für jede Zugangskontroll-Regel kann ein Zeitfenster aktiviert werden. Auf dieser Seite können Sie die Zeitregeln definieren und anschließend der Zugangskontroll-Seite zuweisen.

Erkennung von Hacker-Angriffen/Intrusion Detection:


PHILIPS
SECURITY
SETUP WIZARD
ADSL / Internet Settings
Security
Firewall
Access Control
MAC Filter
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
Wireless
Home Network Settings
Advanced Settings
Intrusion Detection
When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Device will support full operation as initiated from the local LAN.
The Device firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.
Intrusion Detection Feature
SPI and Anti-DoS firewall protection
RIP defect
Discard Ping To WAN Interface
Stateful Packet Inspection
Packet Fragmentation
TCP Connection
UDP Session
FTP Service
H.323 Service
TFTP Service
When hackers attempt to enter your network, the router can alert you by e-mail
Your E-mail Address
SMTP Server Address
POP3 Server Address
User name
Password
Connection Policy
Fragmentation half-open wait
TCP SYN wait
TCP FIN wait
TCP connection idle timeout
UDP session idle timeout
H.323 data channel idle timeout
DoS Detect Criteria
Total incomplete TCP/UDP sessions HIGH
Total incomplete TCP/UDP sessions LOW
Incomplete TCP/UDP sessions (per min) HIGH
Incomplete TCP/UDP sessions (per min) LOW
Maximum incomplete TCP/UDP sessions number from same host
Incomplete TCP/UDP sessions detect sensitive time period
Maximum half-open fragmentation packet number from same host
Half-open fragmentation detect sensitive time period
Flooding cracker block time
SAVE SETTINGS
CANCEL

Erkennung von Hacker-Angriffen

Filterung durch Status der Datenpakete (Stateful Packet Inspection - SPI) und Anti-DoS Firewall Schutz (standardmäßig aktiviert) - Die Funktion "Erkennung von Hacker-Angriffen" auf der ADSL-WLAN-Basisstation grenzt den Zugang des ankommenden Datenverkehrs auf dem WAN-Port ein. Wenn die SPI-Funktion aktiviert ist, werden alle ankommenden Datenpakete abgeblockt mit Ausnahme der Paketarten, die im Feld "Filterung durch Status der Datenpakete" als zugelassen markiert wurden.

RIP Defekt (standardmäßig deaktiviert) - Wenn ein Paket mit RIP-Anforderung vom Router nicht zugelassen wird, bleibt es in der Eingangswarteschleife und wird nicht freigegeben. Angesammelte Pakete können die Eingangswarteschleife überfüllen und gravierende Probleme bei allen Protokollen verusachen. Das Aktivieren dieser Funktion verhindert das Ansammeln von Paketen.

Ping zum WAN nicht zulassen (standardmäßig deaktiviert) - Verhindert, dass der Ping vom Port der ADSL-WLAN-Basisstation an das Netzwerk weitergeleitet wird.

Scrollen Sie nach unten, um weitere Informationen anzuzeigen.

Stateful Packet Inspection (Filterung durch Status der Datenpakete)

Das Filtern der Datenpakete durch SPI wird so genannt, weil der Inhalt der Datenpakete geprüft wird, um den Zustand der Kommunikation zu ermitteln; es prüft z.B., dass der ausgewiesene Zielcomputer die aktuelle Kommunikation zuvor angefordert hat. Dies ist eine Möglichkeit, um sicherzustellen, dass alle Kommunikationen vom Empfängercomputer initiiert wurden und mit durch vorherige Verbindungen bekannten und vertrauenswürdigen Quellen stattfinden. Neben der strengeren Kontrolle der Pakete schließen statusabhängige Firewalls die Ports, bis der Zugang zu diesen Ports angefragt wird.

Wenn spezielle Arten des Datenverkehrs überprüft werden, wird nur die Datenverkehrart zugelassen, die vom internen, lokalen Netz freigegeben ist. Hat der Benutzer z.B. im Bereich "Stateful Packet Inspection" die Schaltfläche "FTP Service" aktiviert, werden alle ankommenden Daten geblockt mit Ausnahme der vom lokalen LAN initiierten FTP-Verbindungen.

Mit "Stateful Packet Inspection" können Sie verschiedene Arten von Anwendungen auswählen, die dynamische Portbezeichnungen verwenden. Wenn Sie Stateful Packet Inspection (SPI) verwenden möchten, um Pakete zu blocken, klicken Sie auf die Schaltfläche "Yes" im Feld "Enable SPI and Anti-DoS firewall protection" und wählen Sie dann die gewünschte Prüfungsart wie z.B. Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service oder TFTP Service.

Versucht ein Hacker in Ihr Netzwerk einzudringen, kann der Router Sie via E-Mail benachrichtigen

Benötigt Ihr E-Mail-Server zum Senden von E-Mails Ihre Authentifizierung, tragen Sie die entsprechenden Informationen in den Feldern POP3-Server, Benutzername und Kennwort ein. Andernfalls lassen Sie diese Felder frei.

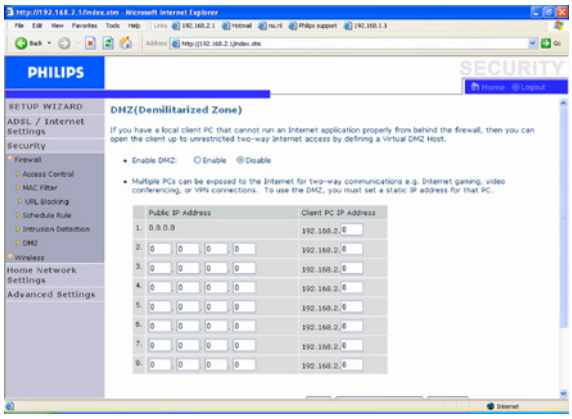
Verbindungsüberwachung

Geben Sie die entsprechenden Werte für TCP / UDP-Sitzungen wie in nachfolgender Tabelle beschrieben ein.

Hinweis

Die Firewall beeinträchtigt die Systemleistung nur geringfügig, deswegen empfehlen wir die Schutzfunktionen zur Absicherung Ihres Netzwerkes aktiviert zu lassen.

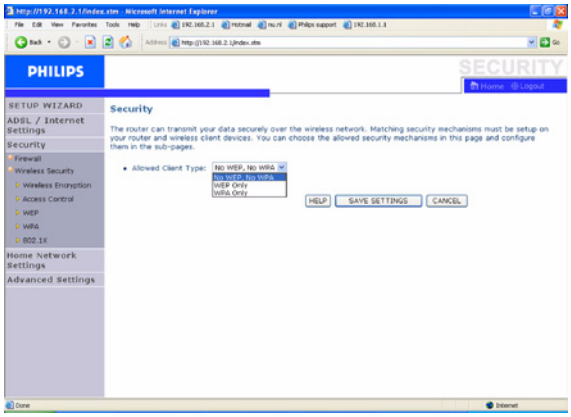
DMZ:


PHILIPS
SECURITY
SETUP WIZARD
ADSL / Internet Settings
Security
Firewall
Access Control
MAC Filter
URL Blocking
Schedule Rule
Intrusion Detection
DMZ
Wireless
Home Network Settings
Advanced Settings
DMZ(Demilitarized Zone)
If you have a local client PC that cannot run an Internet application properly from behind the firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.
Enable DMZ:
Enable
Disable
Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.
Public IP Address
Client PC IP Address
0.0.0.0
192.168.2.0

Verwenden Sie einen Client-PC, der nicht in der Lage ist, eine Internetanwendung bei aktivierter Firewall zu starten, können Sie den Client für den unbegrenzten, wechselseitigen Internetzugang öffnen. Geben Sie in diesem Bildschirmfenster die IP-Adresse eines DMZ (entmilitarisierte Zone) -Hosts ein. Wenn Sie dieser DMZ einen Client hinzufügen, kann Ihr lokales Netzwerk einer Vielzahl von Sicherheitsrisiken ausgesetzt sein. Verwenden Sie diese Option deshalb nur, wenn es keine andere Lösung gibt.

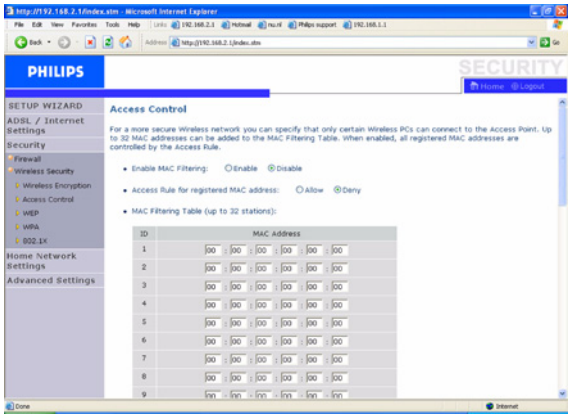
4.4.2 WLAN Sicherheit/Wireless Security

WLAN Verschlüsselung/Wireless Encryption:



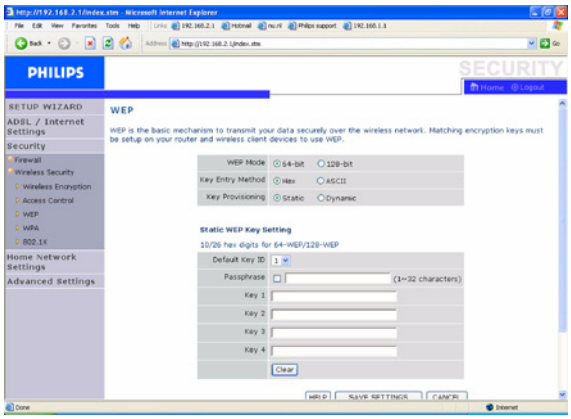
Um Ihr WLAN-Netzwerk abzusichern, sollten Sie die Schutzfunktion aktivieren. Die ADSL-WLAN-Basisstation unterstützt die WEP- (Wired Equivalent Privacy), WPA- (Wi-Fi Protected Access) und die 802.1x-Schutzmechanismen. Es ist höchst ratsam die WPA-Schutzfunktion einzusetzen.

Zugangskontrolle/Access Control:



Die Zugangskontrolle ermöglicht den Benutzern den erlaubten oder nicht erlaubten abgehenden Datenverkehr über die WAN-Schnittstelle zu definieren. Standardmäßig ist der gesamte abgehende Datenverkehr zugelassen.

WEP:



Wenn Sie Ihr WLAN-Netzwerk mit WEP absichern möchten, müssen Sie für die ADSL-WLAN-Basisstation und für alle anderen WLAN-Clients die gleichen Parameter einstellen.

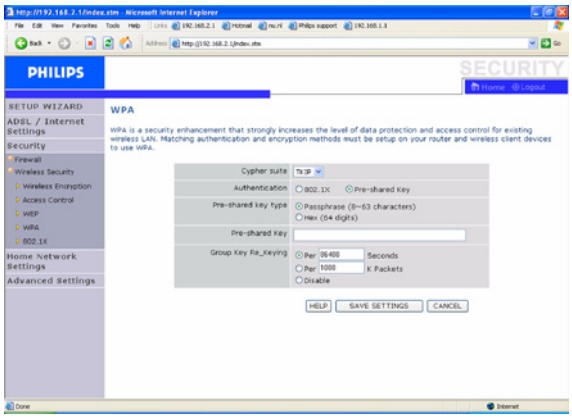
Die Verschlüsselungen können entweder automatisch oder manuell durch Eingabe des Schlüsselwortes generiert werden. Um die Verschlüsselung automatisch mit einem Passwortsatz zu generieren, aktivieren Sie die Schaltfläche “Passphrase” und geben Sie die Zeichenkette ein. Wählen Sie im Aufklappmenü die Standardverschlüsselung aus. Klicken Sie auf “SAVE SETTINGS”.

Hinweis

Der Passwortsatz kann aus 32 alphanumerischen Zeichen zusammengesetzt werden.

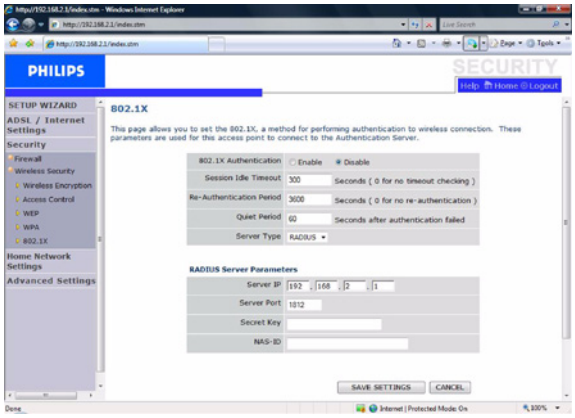
Um die Verschlüsselung manuell zu konfigurieren, geben Sie fünf hexadezimale Zeichenpaare für jeden 64-Bit Schlüssel ein, oder 13 Paare für den 128-Bit Einzelschlüssel.
(Ein hexadezimales Zeichen ist eine Zahl oder ein Buchstabe im Bereich von 0–9 oder A–F).
Beachten Sie, dass WEP zwar die Daten schützt, die zwischen den drahtlosen Knotenpunkten ausgetauscht werden, jedoch nicht die Daten, die über Ihr verkabeltes Netzwerk oder das Internet übertragen werden.

WPA:



Der geschützte WiFi-Zugang [Wi-Fi Protected Access] (WPA) kombiniert das Temporal Key Integrity Protocol (TKIP) und die 802.1x-Mechanismen. Er enthält eine dynamische Verschlüsselung und einen 802.1x-Authentifizierungsdienst.

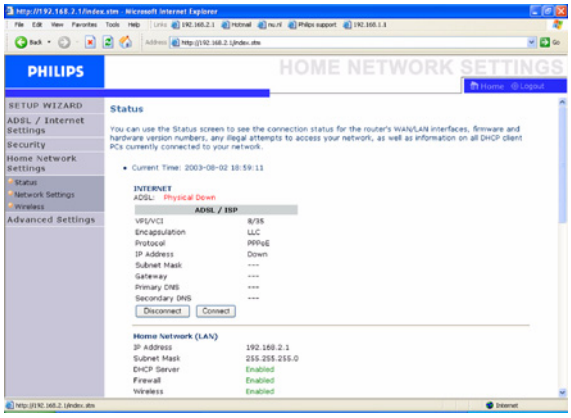
802.1x:



Verwenden Sie in Ihrem Netzwerk die 802.1x-Technologie, sollten Sie diese Funktion für die ADSL-WLAN-Basisstation aktivieren. Diese Parameter werden für die ADSL-WLAN-Basisstation benötigt, um die Verbindung mit dem Authentifizierungsserver herzustellen.

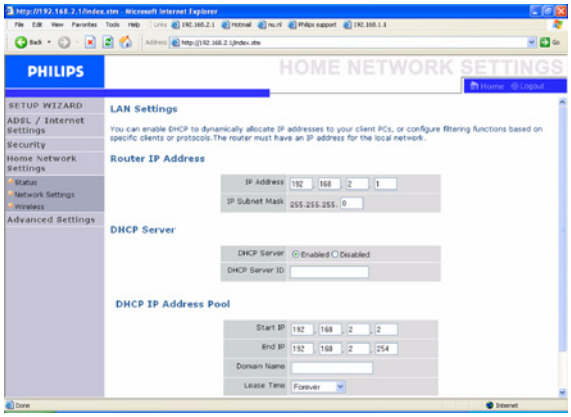
4.5 Webseiten zur Einstellung von Heimnetzwerken

4.5.1 Status



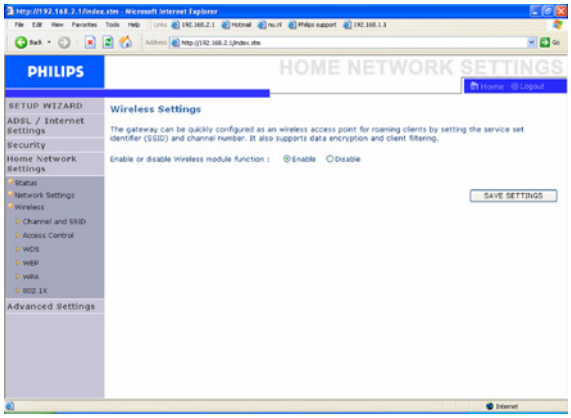
Die Statusseite zeigt den Status der WAN- / LAN-Verbindung an, die Firmware und die Versionsnummer der Hardware, illegale Zugriffsversuche auf Ihr Netzwerk sowie Informationen zu den DHCP-Clients, die mit Ihrem Netzwerk verbunden sind. Das Sicherheitsprotokoll kann als Datei gespeichert werden, indem man auf “Save” klickt und einen Speicherort auswählt.

4.5.2 Netzwerk-Einstellungen/Network settings



Verwenden Sie das Menü “Home Networking” zur Konfiguration der LAN-IP-Adresse und zur Aktivierung des DHCP-Servers für die Zuweisung der dynamischen Clientadresse.

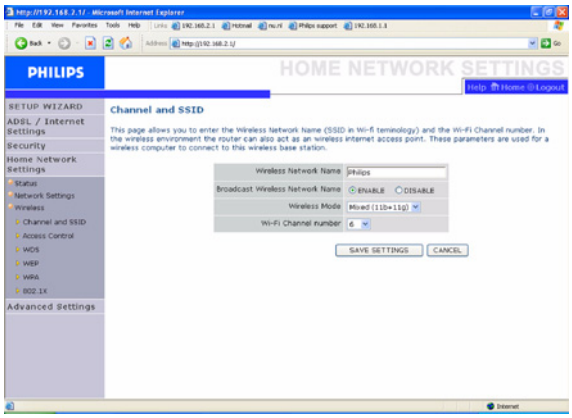
4.5.3 Drahtlos (WLAN)/Wireless



Die ADSL-WLAN-Basisstation fungiert auch als WLAN-Access-Point, dadurch können Computer drahtlos miteinander kommunizieren.

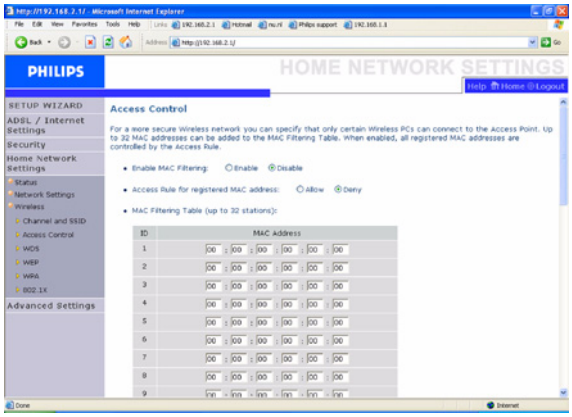
Um dieses Leistungsmerkmal zu konfigurieren, müssen Sie die WLAN-Funktion aktivieren sowie den Funkkanal, die Kennung der Domäne und die Sicherheitsoptionen definieren.
Aktivieren Sie die Schalfläche “Enable” und klicken Sie auf “SAVE SETTINGS”.

Kanal und SSID/Channel and SSID:



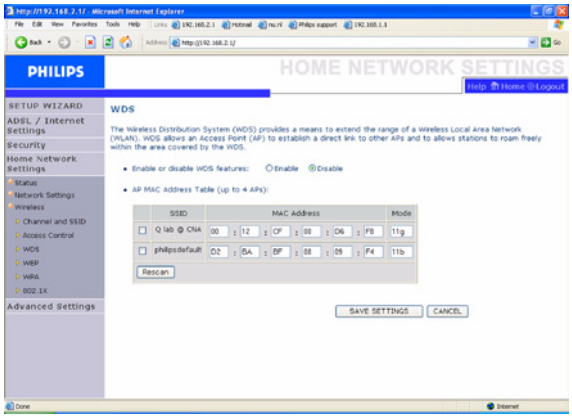
Sie müssen einen einheitlichen Funkkanal und eine einheitliche SSID (Service Set ID) bestimmen, der / die von der ADSL-WLAN-Basisstation und allen drahtlosen Clients verwendet wird. Stellen Sie sicher, dass Sie alle Clients mit den gleichen Werten konfiguriert haben.

Zugangskontrolle/Access Control:



Mit der Zugangskontrolle (Access Control) kann der Benutzer Berechtigungen für den abgehenden Datenverkehr über die WAN-Schnittstelle definieren. Standardmäßig ist der abgehende Datenverkehr uneingeschränkt zugelassen.

WDS:



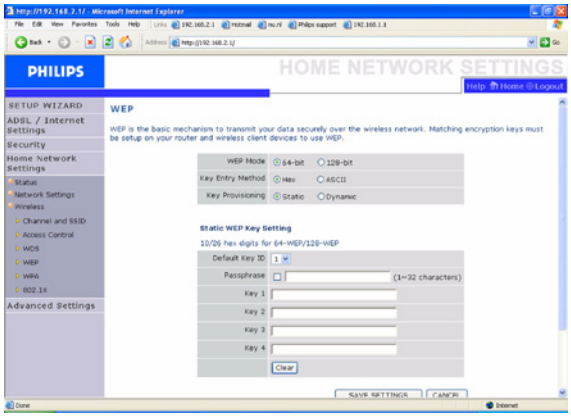
Wenn die Signalstärke einer im Netzwerk eingebundenen WLAN-Basisstation aufgrund eines großen Abdeckungsbereiches oder wegen Beeinträchtigung durch Wände nicht ausreicht, kann die Reichweite dieser Basisstation mittels WDS erweitert werden.

Alle Basisstationen innerhalb eines WDS müssen mit dem gleichen Funkkanal und, falls benötigt, mit der gleichen Verschlüsselungsart (WEP / WPA) konfiguriert werden.

Hinweis

Die WDS-Funktionalität ist in den IEEE- oder WiFi-Richtlinien nicht vollständig spezifiziert. Demzufolge kann nicht gewährleistet werden, dass WDS mit Produkten anderer Hersteller funktioniert.

WEP:



Wenn Sie WEP zum Schutz Ihres WLAN-Netzwerkes verwenden, müssen Sie für die ADSL-WLAN-Basisstation und alle WLAN-Clients die gleichen Parameter einstellen.

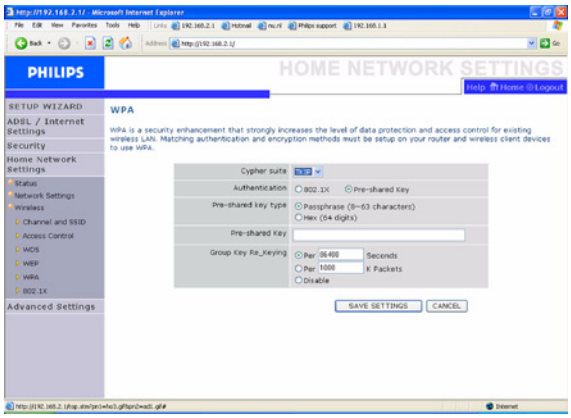
Die Verschlüsselungen können entweder automatisch oder manuell durch Eingabe des Schlüsselwortes generiert werden. Um die Verschlüsselung automatisch mit einem Passwortsatz zu generieren, aktivieren Sie die Schaltfläche "Passphrase" und geben Sie die Zeichenkette ein. Wählen Sie im Aufklappmenü die Standardverschlüsselung aus. Klicken Sie auf "SAVE SETTINGS".

Hinweis

Der Passwortsatz kann aus 32 alphanumerischen Zeichen zusammengesetzt werden.

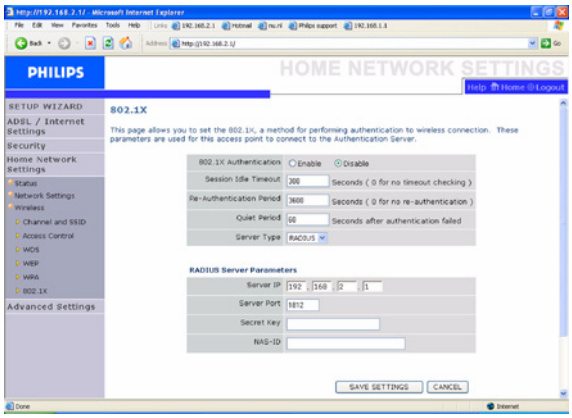
Um die Verschlüsselung manuell zu konfigurieren, geben Sie fünf hexadezimale Zeichenpaare für jeden 64-Bit Schlüssel ein, oder 13 Paare für den 128-Bit Einzelschlüssel.
(Ein hexadezimales Zeichen ist eine Zahl oder ein Buchstabe im Bereich von 0–9 oder A–F).
Beachten Sie, dass WEP zwar die Daten schützt, die zwischen den drahtlosen Knotenpunkten ausgetauscht werden, jedoch nicht die Daten, die über Ihr verkabeltes Netzwerk oder das Internet übertragen werden.

WPA:



Der geschützte WiFi-Zugang (WPA) kombiniert das TKIP-Protokoll (Temporal Key Integrity Protocol) mit den 802.1x-Mechanismen. Er umfasst eine dynamische Verschlüsselung und einen 802.1x-Authentifizierungsdienst.

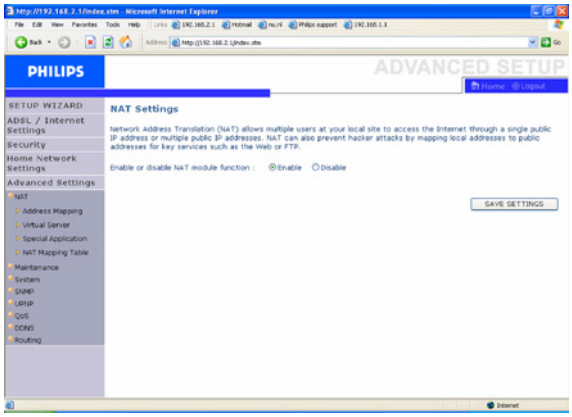
802.1x:



Wenn Sie in Ihrem Netzwerk die 802.1x-Technologie verwenden, sollten Sie diese Funktion für die ADSL-WLAN-Bassisstation aktivieren. Diese Parameter werden für die ADSL-WLAN-Basisstation benötigt, um die Verbindung zum Authentifizierungsserver herzustellen.

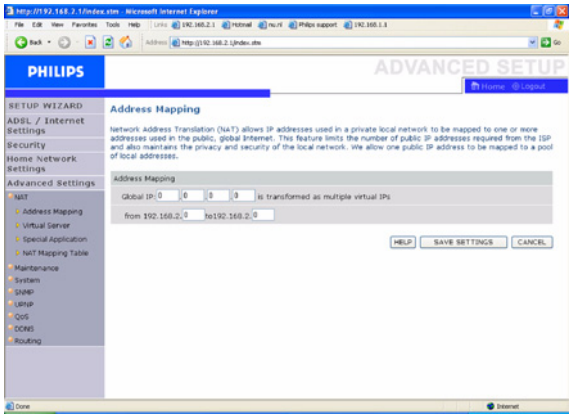
4.6 Webseiten für erweiterte Einstellungen/Advanced settings webpages

4.6.1 NAT



Das NAT (Network Address Translation) ermöglicht mehreren Benutzern den Zugang zum Internet mit einer gemeinsamen IP-Adresse.

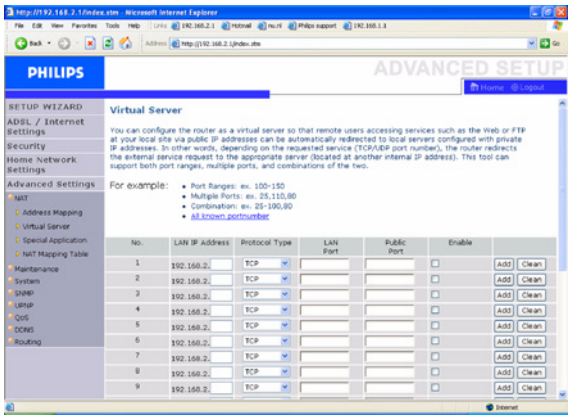
Adressen-Mapping/Address Mapping:



Eine oder mehrere öffentliche IP-Adressen können von mehreren internen Benutzern benutzt werden. Dabei wird das interne Netz maskiert, was einen besseren Datenschutz und eine höhere Sicherheit bietet.

Geben Sie die gemeinsame öffentliche IP-Adresse in das Feld “Global IP” ein. Geben Sie in das Feld “from” eine Reihe von internen IP-Adressen für die gemeinsame Nutzung der IP-Adresse ein.

Virtueller Server/Virtual Server:

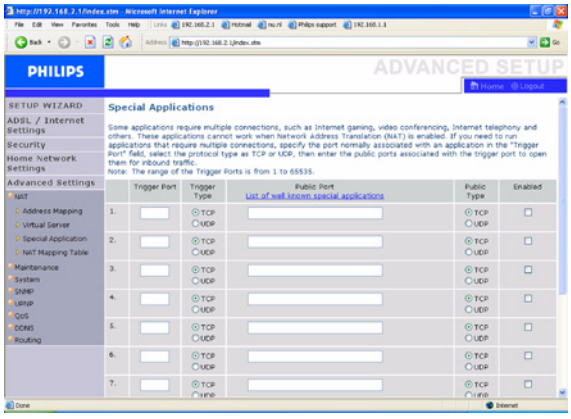


Werden über die ADSL-WLAN-Basisstation virtuelle Server konfiguriert, können externe Benutzer, die auf deren Dienste zugreifen, z.B. Internet oder FTP auf der lokalen Einrichtung über öffentliche IP-Adressen, automatisch an lokale Server weitergeleitet werden, die mit privaten IP-Adressen konfiguriert sind. Das heißt: abhängig von den angeforderten Diensten (TCP / UDP Portnummer) leitet die ADSL-WLAN-Basisstation die externe Dienstanforderung an den entsprechenden Rechner weiter (der unter einer anderen IP-Adresse zu erreichen ist).

Wenn Sie z.B. die Einstellung TCP/80 (HTTP oder Web) als “Typ / Öffentliches Port” und 192.168.2.2/80 als “Private IP / Port” einstellen, werden alle HTTP-Anfragen von externen Benutzern nach 192.168.2.2 an das Port 80 weitergeleitet. Deshalb können Internetbenutzer durch Eingabe der vom Internet-Provider bereitgestellten IP-Adresse den gewünschten Dienst über die lokale Adresse nutzen, an die Sie sie weiterleiten.

Eine Liste der Ports finden Sie unter nachfolgendem Link:
http://www.iana.org/assignments/port-numbers

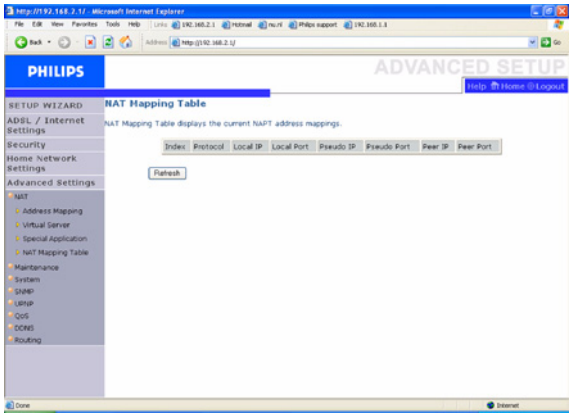
Spezielle Anwendungen/Special Applications:



Einige Anwendungen erfordern mehrfache Verbindungen, wie z.B. Internetspiele, Videokonferenzen und Internettelefonie.

Diese Anwendungen funktionieren eventuell nicht, wenn NAT (Network Address Translation) aktiviert ist. Werden Anwendungen eingesetzt, die mehrfache Verbindungen benötigen, verwenden Sie diese Seiten, um die zusätzlichen öffentlichen Ports für die einzelnen Anwendungen zu spezifizieren.

Tabelle NAT-Mapping/NAT Mapping Table:

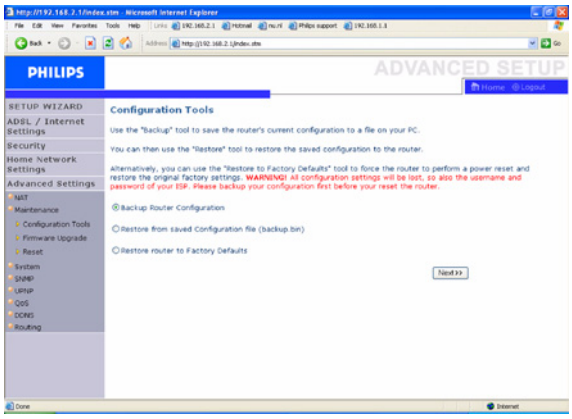


Diese Seite zeigt das aktuelle NAPT (Network Address Port Translation) Adressen-Mapping.

4.6.2 Instandhaltung/Maintenance

Verwenden Sie das Instandhaltungs-Menü zum Speichern der aktuellen Konfiguration, z.B. um eine zuvor gespeicherte Konfiguration wiederherzustellen, die Werkseinstellungen wiederherzustellen, die Firmware zu aktualisieren oder, um die ADSL-WLAN-Basisstation zurückzusetzen.

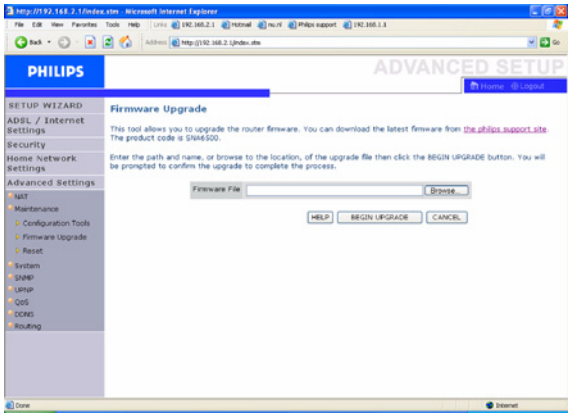
Konfigurations-Werkzeuge/Configuration Tools:



Wählen Sie eine Funktion aus und klicken Sie auf “**Next>>**”.

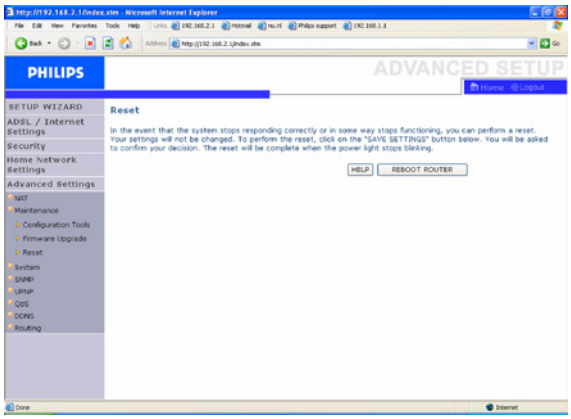
Mit der Funktion “Backup” kann die Konfiguration der ADSL-WLAN-Basisstation in einer Datei gespeichert werden.
Die Funktion “Restore” kann zur Wiederherstellung der gespeicherten Backupkonfiguration verwendet werden.
“Restore to Factory Defaults” setzt die ADSL-WLAN-Basisstation auf die Werkseinstellungen zurück. Sie werden aufgefordert, das Zurücksetzen zu bestätigen.

Aktualisierung der Firmware/Firmware Upgrade:



Verwenden Sie das Bildschirmfenster "Firmware Upgrade", um die Firmware oder Benutzeroberfläche auf die neueste Version zu aktualisieren. Laden Sie die Upgrade-Datei von www.philips.com/support (für das Modell CGA5722) herunter und speichern Sie diese auf Ihrer Festplatte. Klicken Sie dann auf "Browse...", um die heruntergeladene Datei zu suchen. Klicken Sie auf "BEGIN UPGRADE". Prüfen Sie die Informationen auf der Statusseite, um sicherzustellen, dass die Aktualisierung erfolgreich war.

Zurücksetzen/Reset:

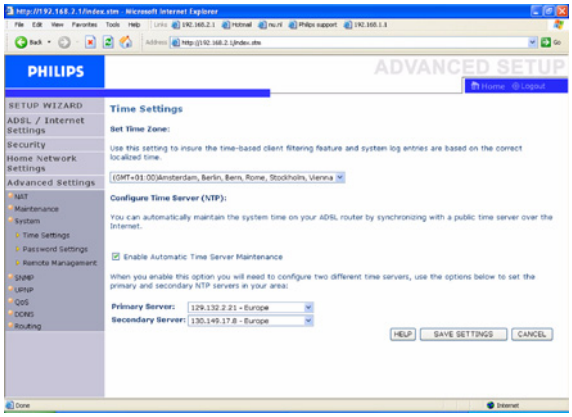


Klicken Sie auf "REBOOT ROUTER", um die ADSL-WLAN-Basisstation zurückzusetzen.
Wenn Sie das Zurücksetzen von dieser Webseite aus starten, wird die Konfiguration nicht auf die Werkseinstellungen zurückgesetzt.

Hinweis
Wenn Sie den Reset-Knopf auf der Rückseite der ADSL-WLAN-Basisstation drücken, wird die Basisstation neu gestartet. Wenn Sie den Reset-Knopf für mehr als 5 Sekunden gedrückt halten, werden die Werkseinstellungen wiederhergestellt.

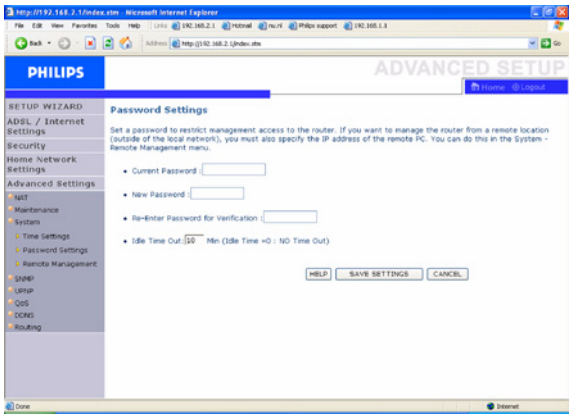
4.6.3 System

Zeit-Einstellungen/Time Settings:



Wählen Sie in der Aufklappliste Ihre lokale Zeitzone aus. Diese Information wird für Protokolleinträge und die Filterung der Clients benötigt.
Wenn Sie möchten, dass die ADSL-WLAN-Basisstation automatisch mit einem öffentlichen Zeitserver synchronisiert wird, aktivieren Sie die Schaltfläche "Enable Automatic Time Server Maintenance". Wählen Sie dann die gewünschten Server im Aufklappmenü aus.

Passwort-Einstellungen/Password Settings:



Verwenden Sie diese Seite, um das Passwort für den Zugriff auf die Verwaltungsoberfläche der ADSL-WLAN-Basisstation zu ändern.

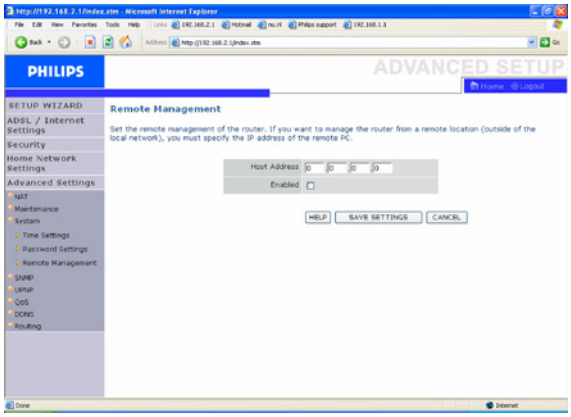
Das Passwort kann aus 3-12 alphanumerischen Zeichen bestehen, es wird zwischen Groß- und Kleinbuchstaben unterschieden.

Hinweis
Sollten Sie Ihr Passwort vergessen haben oder keinen Zugriff auf die Benutzeroberfläche haben, halten Sie den blauen Reset-Knopf auf der Rückseite des Gerätes für mindestens fünf Sekunden gedrückt, um die Werkseinstellungen wiederherzustellen. Wenn die Werkseinstellungen aktiviert sind, wird kein Passwort für den Zugriff auf die Benutzeroberfläche benötigt.

Achtung
Beim Zurücksetzen (Reset) der ADSL-WLAN-Basisstation mit dem Reset-Knopf gehen alle Konfigurations- und IP-Einstellungen (Internet-Provider) verloren.

Geben Sie die maximale Dauer der Inaktivität (in Minuten) ein; damit wird die maximale Zeitspanne definiert, die eine Login-Sitzung bei Inaktivität aufrechterhalten werden soll. Bleibt die Verbindung länger inaktiv als die vorgegebene maximale Inaktivitätszeit, erfolgt automatisch ein Systemlogout. Sie müssen sich dann erneut einloggen, um auf die Verwaltungsoberfläche zugreifen zu können (Standardeinstellung: 10 Minuten).

Fernverwaltung/Remote Management:



Standardmäßig können nur die Benutzer Ihres lokalen Netzwerkes auf den Verwaltungsbereich zugreifen. Sie können jedoch die ADSL-WLAN-Basisstation auch von einem entfernten Host fernverwalten, indem Sie die IP-Adresse eines externen Computers in dieses Bildschirmfenster eingeben. Aktivieren Sie die Schaltfläche "Enabled", geben Sie die IP-Adresse des Hosts ein und klicken Sie auf "SAVE SETTINGS".

Hinweis

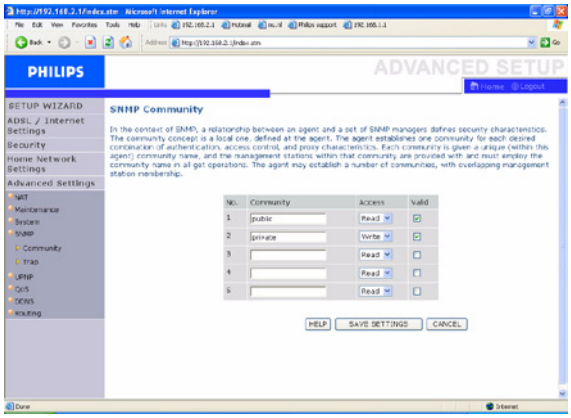
Wenn Sie die Schaltfläche "Enable" aktivieren und als IP-Adresse 0.0.0.0 angeben, kann die ADSL-WLAN-Basisstation von jedem beliebigen, externen Host verwaltet werden.

Für die Fernverwaltung über die WAN-IP-Adresse müssen Sie eine Verbindung über Port 8080 herstellen. Geben Sie einfach die WAN-IP-Adresse gefolgt von 8080 ein, z.B. 212.120.68.20:8080.

4.6.4 SNMP

Verwenden Sie das SNMP-Konfigurationsfenster, um die Parameter für das SNMP-Protokoll (Simple Network Management Protocol) anzuzeigen und zu ändern.

SNMP Gemeinschaft/SNMP community:



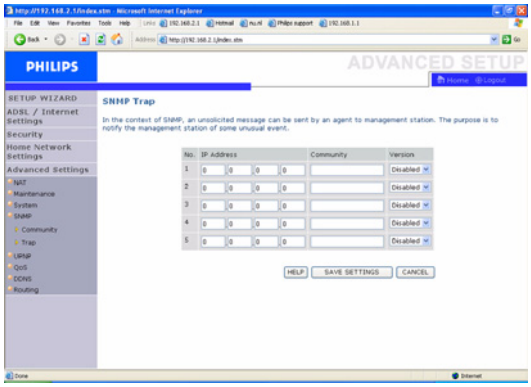
Sie können einen im Netzwerk integrierten Computer, eine sogenannte Network Management Station (NMS), verwenden, um auf diese Informationen zuzugreifen. Die Zugangsrechte werden von den Community Strings kontrolliert. Um mit der ADSL-WLAN-Basisstation kommunizieren zu können, muss die NMS zuerst einen gültigen Community String zur Authentifizierung vorweisen.

Parameter	Beschreibung
Gemeinschaft/ Community	Ein Gemeinschafts-Name für den berechtigten Zugriff auf die Verwaltung
Zugriff/Access	Der Zugriff auf die Verwaltung ist begrenzt auf Nur lesen (lesen) oder Lesen / Schreiben (schreiben)
Bestätigung/Valid	Eingabe aktivieren/deaktivieren

Hinweis

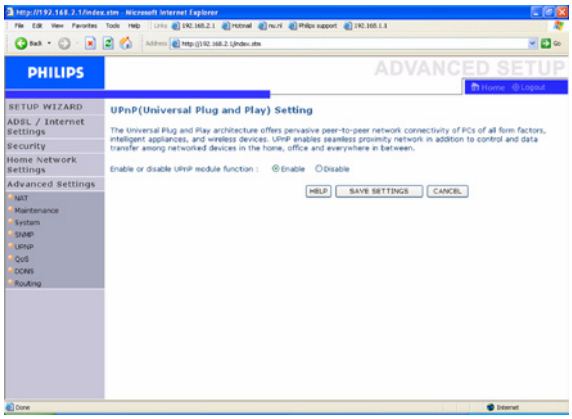
Es können bis zu fünf Gemeinschafts-Namen eingegeben werden.

SNMP Trap:



Spezifizieren Sie die IP-Adresse der NMS, damit vom Agenten erkannte, besondere Ereignisse gemeldet werden. Wenn Bedingungen für eine Gefahr ermittelt wurden, sendet der SNMP-Agent eine SNMP-Gefahrenmeldung an jeden NMS-spezifizierten Empfänger.

4.7 UPNP



UPNP (Universal Plug and Play) Einstellungen

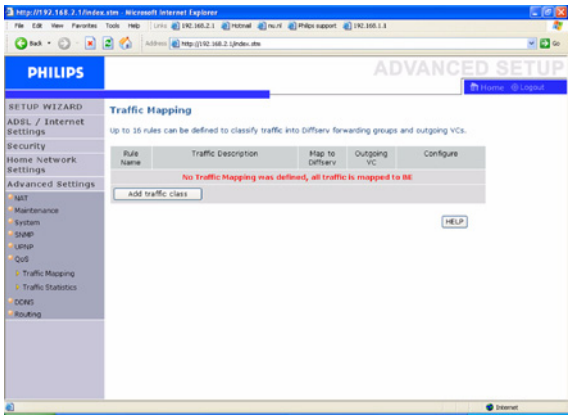
Mit Universal Plug and Play kann sich ein Gerät automatisch in ein Netzwerk einloggen, eine IP-Adresse erhalten, seine Leistungsfähigkeit vermitteln und Informationen über die Anwesenheit und die Leistungsfähigkeit anderer Geräte abfragen. Die Geräte können dann direkt miteinander kommunizieren. Dies ermöglicht desweiteren den Aufbau eines Peer-to-Peer-Netzes (Punkt zu Punkt).

4.8 QoS

Auf der Seite mit den QoS-Einstellungen kann der Benutzer die Konfiguration der Bandbreitenzuweisung für jede Übertragungsart definieren. Die QoS-Einstellungen sind nachfolgend beschrieben:

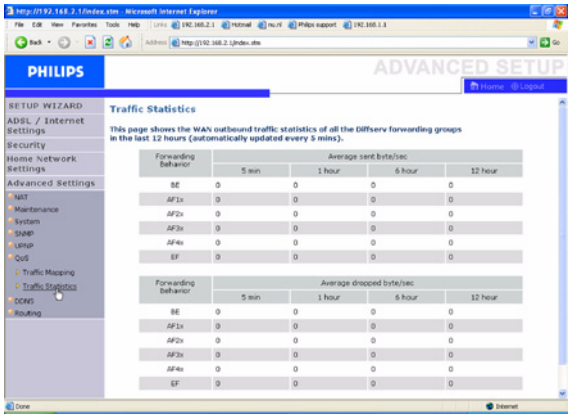
“Name” - Zeigt den Namen der Übertragungsart an, z.B. Best Effort, Assured Forwarding oder Expedited Forwarding.
“Description” - Kurze Beschreibung der verwendeten Übertragungsart.
“Priority” - “Best Effort” hat die niedrigste Priorität, da es sich um einen Standard-Konnektivitätsdienst handelt mit keinerlei Garantien.
“Expedited Forwarding” hat die höchste Priorität. Es bietet die geringste Verzögerung und Aperturunsicherheit sowie einen geringen Verlust der abgelieferten Pakete.
“Bandwidth Allocation” - Sie wählen die minimale Bandbreite für jede Übertragungsmethode aus.

Mapping des Datenverkehrs/Traffic Mapping:



Mit “Traffic Mapping” können Sie bis zu 16 Regeln festlegen zur Klassifizierung des Datenverkehrs in Übermittlungsgruppen. Sie müssen die Datenverkehrsart, die Übertragungsmethode und die abgehende virtuelle Verbindung (VC - Virtual Connection) spezifizieren, an die dieser Datenverkehr weitergeleitet wird.

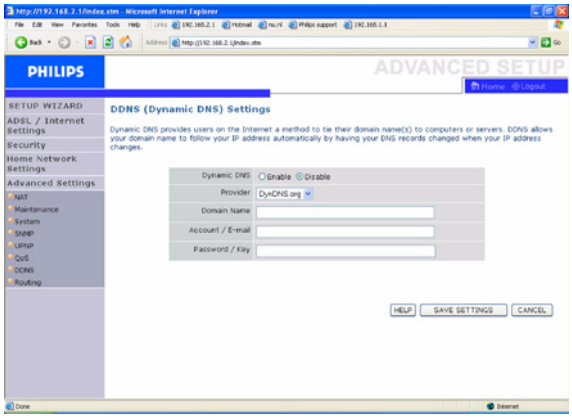
Statistik des Datenverkehrs/Traffic Statistics:



Das Bildschirmfenster der Statistik des Datenverkehrs zeigt die abgehenden Verkehrsstatistiken von allen Übertragungsmethoden über einen Zeitraum von 12 Stunden.

4.9 DDNS

DDNS (Dynamische DNS) Eintellungen/DDNS (Dynamic DNS) settings



Der DDNS-Text “Domain Name” ist eine Kette alphanumerischer, durch Punkte abgetrennter Zeichen, die an die Adresse einer Netzwerkverbindung angehängt wird und den Eigentümer der Adresse identifiziert.

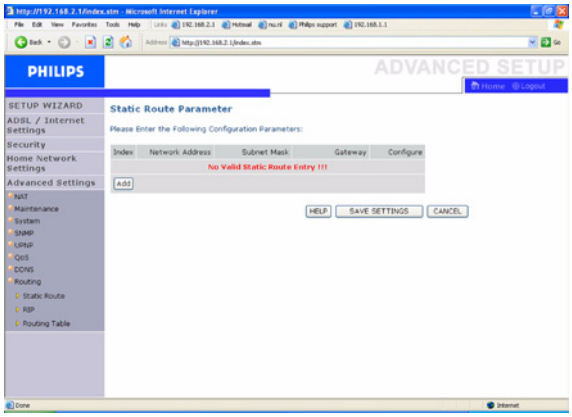
Die dynamische DNS stellt den Benutzern im Internet eine Methode zur Verfügung, um ihren Domänen-Namen an einen Computer oder Server zu binden. Mit DDNS ist es möglich, dass Ihr Domänen-Name automatisch an Ihre IP-Adresse angehängt wird, indem Ihre DNS-Einträge aktualisiert werden, wenn sich Ihre IP-Adresse ändert.
Der Abschnitt “Server Konfiguration” öffnet automatisch die TCP-Portoptionen, die im Abschnitt “Virtueller Server” aktiviert wurden. Geben Sie einfach die IP-Adresse Ihres Servers ein, wie bei einem Webserver, und klicken Sie dann auf die Portoption HTTP Port 80, damit die Benutzer über die Internetverbindung auf Ihren Webserver zugreifen können.

Diese DNS-Funktion wird von einem DDNS-Service-Provider unterstützt. Mit einer DDNS-Verbindung können Sie Ihre eigene Web-Seite, Ihren E-Mail-Server, Ihre FTP-Seiten und vieles mehr über Ihr eigenes Netz einrichten. (Standardeinstellung: Deaktiviert)

4.10 Routing

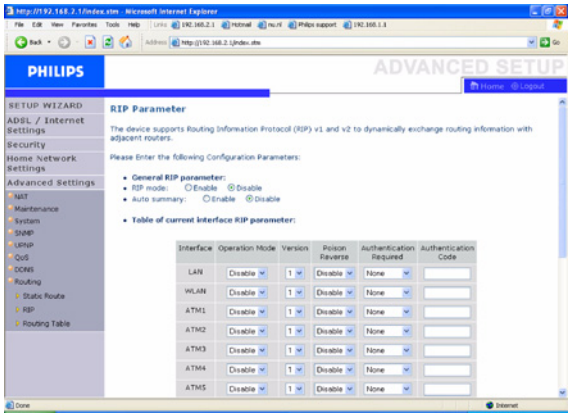
Diese Seiten definieren routingbezogene Parameter, inklusive feste Routen und RIP (Routing Information Protocol) Parameter.

Feste Route/Static route:



1- Klicken Sie auf “Add”, um eine neue, feste Route in der Liste einzufügen
2- Klicken Sie auf “Save Settings”, um die Konfiguration zu speichern

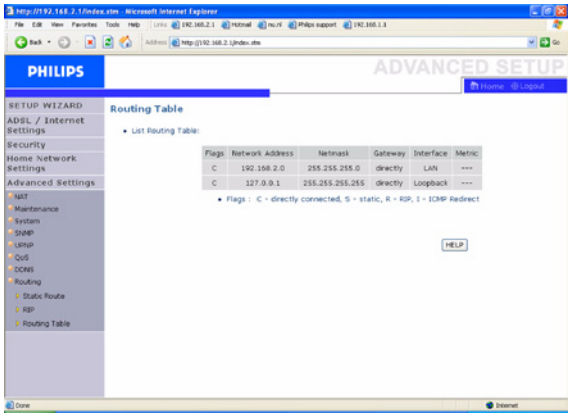
RIP Parameter/RIP parameters:



RIP sendet nicht nur in regelmäßigen Intervallen Routing-Update-Benachrichtigungen, sondern auch, wenn sich die Netzwerkstruktur ändert. Erhält ein Router ein Routing-Update mit einer Veränderung eines Eintrages, wird die Routingtabelle entsprechend aktualisiert und die neue Route berücksichtigt. RIP-Router gewährleisten immer die beste Route zum Zielort.

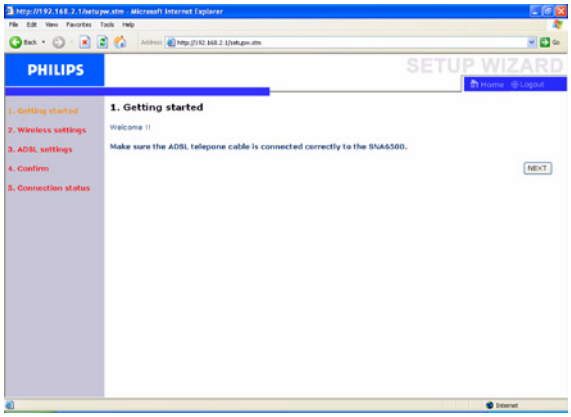
Nach der Aktualisierung seiner Routingtabelle beginnt der Router sofort mit der Übertragung der Updates, um die Änderungen an weitere im Netzwerk befindliche Router weiterzugeben.

Routing Tabelle/Routing table:



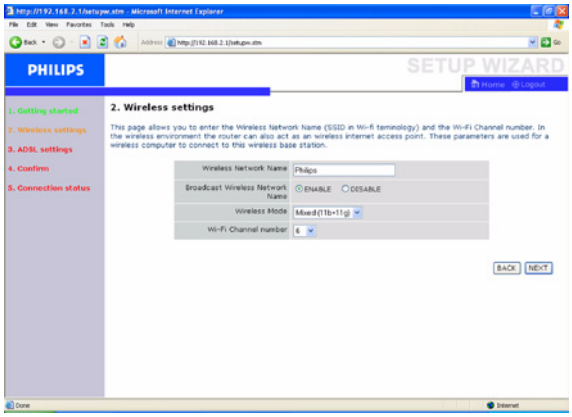
4.11 INSTALLATIONS-ASSISTENT/SET UP WIZARD

Inbetriebnahme/Getting started:



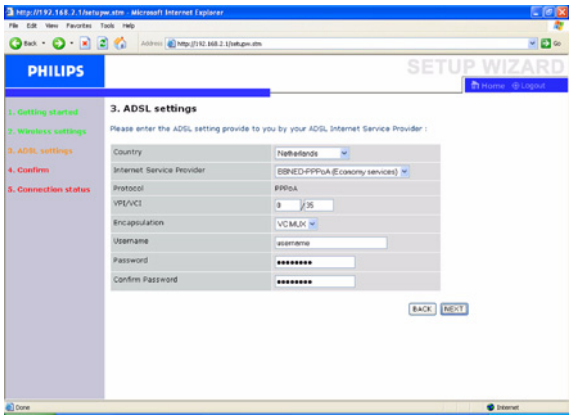
Stellen Sie sicher, dass Sie einen funktionierenden ADSL-Vertrag haben und, dass die ADSL-WLAN-Basisstation an der ADSL-Telefonleitung angeschlossen ist. Sie können prüfen, ob das Kabel korrekt angeschlossen ist, indem Sie die ADSL-Kontrollanzeige, oben auf der ADSL-WLAN-Basisstation, beobachten. Die ADSL-Kontrollanzeige sollte nach ca. 1 Minute dauerhaft leuchten.

WLAN Einstellungen/Wireless settings:


PHILIPS
SETUP WIZARD
1. Getting started
2. Wireless settings
3. ADSL settings
4. Confirm
5. Connection status
2. Wireless settings
This page allows you to enter the Wireless Network Name (SSID in Wi-Fi terminology) and the Wi-Fi Channel number. In the wireless environment the router can also act as an wireless internet access point. These parameters are used for a wireless computer to connect to this wireless base station.
Wireless Network Name
Philips
Broadcast Wireless Network Name
ENABLE
DISABLE
Wireless Mode
Mixed(11b+11g)
Wi-Fi Channel number
6
BACK
NEXT

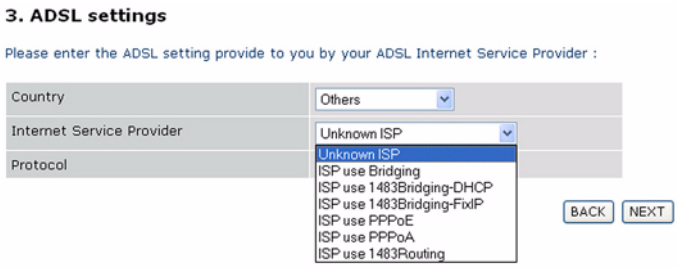
In Schritt 2 können Sie die WLAN-Einstellungen der ADSL-WLAN-Basisstation ändern. Für die einfache Installation wird empfohlen die Standardeinstellungen beizubehalten. Falls Sie die WLAN-Einstellungen zu einem späteren Zeitpunkt ändern möchten, können Sie dafür das Menü der ADSL-WLAN-Basisstation verwenden.

ADSL Einstellungen/ADSL settings:



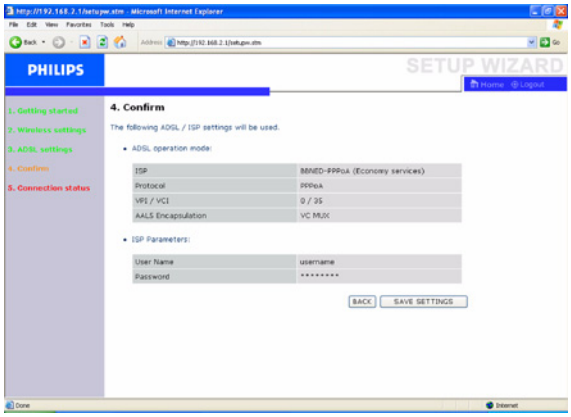
In Schritt 3 müssen Sie die für Ihren ADSL-Internet-Provider (IP) Vertrag zutreffenden Einstellungen eingeben. Bei der einfachen Installation können Sie Ihren IP aus einer Liste vordefinierter ADSL-Provider, landesabhängig, auswählen.

Wenn Sie Ihren IP in der Liste nicht finden können, geben Sie die Einstellungen manuell ein.



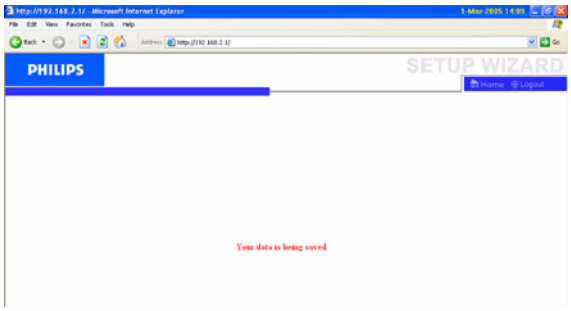
Wählen Sie dafür unter “Country” die Option “others” und wählen Sie in der Liste der “Internet Service Provider” das ADSL-Protokoll aus, das Ihr IP verwendet (diese Angaben finden Sie in den Unterlagen, die Sie von Ihrem IP erhalten haben).

Bestätigen/Confirm:



In Schritt 4 werden die ADSL-Einstellungen, die Sie eingegeben haben und die für die Konfiguration der ADSL-WLAN-Basisstation verwendet werden, angezeigt. Bitte überprüfen Sie diese Einstellungen auf Übereinstimmung mit den Angaben, die in Ihrem ADSL-Vertrag enthalten sind. Möchten Sie Änderungen vornehmen, klicken Sie auf die Schaltfläche “Back” für die Rückkehr zu Schritt 3.

Nachdem Sie auf “SAVE SETTINGS” geklickt haben, erscheint die Meldung “Your data is being saved”.



5 Technische Daten

Ports
- Vier 10/100Mbps Rj-45 Ports
- Ein ADSL RJ-11

ADSL-Funktionen
- Unterstützt die DMT Leitungsmodulation
- Kompatibel mit Annex A Full-Rate ADSL: bis zu 8 Mbps Downstream, bis 1 Mbps Upstream (G.992.1 & TI.143, Ausgabe 2)
- Unterstützt G.Lite ADSL: bis 1.5 Mbps Downstream, bis 512 Kbps Upstream
- Dying GASP-Unterstützung

ATM-Funktionen
- RFC1483 Verkapselung (IP, Bridging und verkapseltes Routing)
- PPP über ATM (LLC & VC Multiplexing) (RFC2364)
- Klassische IP (RFC1577)
- Überwachung Datenverkehr (UBR, CBR)
- OAM F4/F5 Unterstützung
- PPP über Ethernet Client

Verwaltungsfunktionen
- Firmware-Upgrade über Internet-Download
- Verwaltung der Konfigurations-Informationen über das Internet
- Stromvervorgungsanzeigen
- Chronologische Aufzeichnung der Ereignisse und des Datenverlaufs
- Netzwerk-Ping

Sicherheitsfunktionen
- Zugriff auf Konfiguration mit Passwort geschützt
- Benutzer-Authentifikation (PAP/CHAP) mit PPP
- Firewall NAT NAPT
- VPN pass through (IPSec-ESP Tunnel-Modus, L2TP, PPTP)

LAN-Funktionen (lokales Netz)
- IEEE 802.1d (selbst-verbesserndes transparentes Bridging)
- DHCP Server
- DNS Proxy
- Festes Routing, RIPv1 und RIP

Funkleistung
- Frequenzband RF-Modul drahtlos
- 802.11g Funk: 2.4GHz
- 802.11b Funk: 2.4GHz
- Europa - ETSI
- 2412-2472MHz (Ch1~Ch13)

Art der Modulation
- OFDM, CCK

Betriebskanäle konform mit IEEE 802.11b:
- 13 Kanäle (ETSI)

Betriebskanäle konform mit IEEE 802.11g:
- 13 Kanäle (Europa)

RF Output-Leistung Modulationsrate -Output-Leistung (dBm)
- 802.11b - 1Mbps (16dBm)
- 802.11b - 2Mbps (16dBm)
- 802.11b - 5.5Mbps (16dBm)
- 802.11b - 11Mbps (16dBm)

Modulationsrate -Output-Leistung (dBm)
- 802.11g - 6Mbps (15dBm)
- 802.11g - 9Mbps (15dBm)
- 802.11g - 12Mbps (15dBm)
- 802.11g - 18Mbps (15dBm)
- 802.11g - 24Mbps (15dBm)
- 802.11g - 36Mbps (15dBm)
- 802.11g - 48Mbps (15dBm)
- 802.11g - 54Mbps (15dBm)

Modulationsraten-Empfindlichkeit - Empfänger 2.412-2.484 GHz Sensitivität (dBm)
- 802.11b - 1Mbps (90dBm)
- 802.11b - 2Mbps (88dBm)
- 802.11b - 5.5Mbps (85dBm)
- 802.11b - 11Mbps (84dBm)

Geschwindigkeit der Modulation: typische Empfänger-Sensitivität (dBm)
- 802.11g - 6Mbps (88dBm)
- 802.11g - 9Mbps (87dBm)
- 802.11g - 12Mbps (84dBm)
- 802.11g - 18Mbps (82dBm)
- 802.11g - 24Mbps (79dBm)
- 802.11g - 36Mbps (75dBm)
- 802.11g - 48Mbps (68dBm)
- 802.11g - 54Mbps (68dBm)

Umgebung
Konform mit nachfolgenden Richtlinien:

Temperatur: IEC 68-2-14
- 0 bis 50° C (im Betrieb)
- -40 bis 70° C (bei Lagerung)

Feuchtigkeit
- 10% bis 90% (nicht kondensierend)

Vibration
- IEC 68-2-36, IEC 68-2-6

Erschütterung
- IEC 68-2-29

Fall
- IEC 68-2-32

Stromversorgung (Eingang)
- 12V 1A

IEEE-Standards
- IEEE 802.3, 802.3u, 802.11g, 802.1d
- IUT G.dmt
- IUT G.Handshake
- IUT T.413 issue 2 - ADSL full rate

Übereinstimmung mit den Richtlinien für elektromagnetische Kompatibilität
- CE, ETSI, R&TTE, ETS 300 328, ETS 300 826

Sicherheit
- EN 60950

Internet-Standards

- RFC 826 ARP
- RFC 791 IP
- RFC 792 ICMP
- RFC 768 UDP
- RFC 793 TCP
- RFC 783 TFTP
- RFC 1483 AAL5 Datenverkapselung
- RFC 1661 PPP
- RFC 1866 HTML
- RFC 2068 HTTP
- RFC 2364 PPP über ATM

6 Häufig gestellte Fragen

In diesem Kapitel finden Sie häufig gestellte Fragen und Vorschläge für die Problembehebung Ihres WLAN ADSL Modem Routers.

Inbetriebnahme

Ich kann mit dem Internet-Browser keine Verbindung herstellen

- Stellen Sie sicher, dass die Netzwerkverbindung zu Ihrer ADSL WLAN Basisstation funktioniert
- Prüfen Sie alle Parametereinstellungen mit den Angaben Ihres Internet-Providers
- Prüfen Sie die Signale und @

Ich habe mein Passwort vergessen (oder verloren). Wie kann ich meine ADSL-WLAN-Basisstation zurücksetzen (auf die Werkseinstellungen)?

- Stellen Sie sicher, dass die ADSL-WLAN-Basisstation eingeschaltet ist
- Verwenden Sie einen Kugelschreiber, um den vertieften Reset-Knopf auf der Rückseite des Gerätes zu betätigen. Halten Sie den Knopf mindestens fünf Sekunden gedrückt.
- Sobald Sie den Knopf loslassen, wird die ADSL-WLAN-Basisstation neu gestartet

Achtung

Wenn Sie mit dem Reset-Knopf die ADSL-WLAN-Basisstation neu starten, gehen alle Konfigurationseinstellungen verloren, auch Ihre IP-Einstellungen (Internet-Provider).

Ich kann keine WLAN-Verbindung zwischen dem PC und meiner ADSL-WLAN-Basisstation herstellen

- Stellen Sie sicher, dass die WiFi-Funktion auf Ihrer ADSL-WLAN-Basisstation aktiviert ist
- Stellen Sie sicher, dass auf dem PC dieselben SSID-Einstellungen vorgenommen wurden wie auf der ADSL-WLAN-Basisstation. Siehe Webseite “Kanal und SSID/Channel and SSID”.
- Es müssen dieselben Sicherheitseinstellungen auf dem PC und auf der ADSL-WLAN-Basisstation eingerichtet sein. Siehe “Web-Seiten für die Sicherheit”.

Funktionen

Das Signal erscheint nicht

- Stellen Sie sicher, dass der Netzstecker an der Stromversorgung angeschlossen ist
- Stellen Sie sicher, dass der Koaxialstecker des Netzadapters an der Buchse an der ADSL-WLAN-Basisstation angeschlossen ist
- Prüfen Sie, ob die Stromversorgungsanzeige Ihrer ADSL-WLAN-Basisstation leuchtet
- Ist die Stromversorgungsanzeige nach einer Weile immer noch ausgeschaltet, prüfen Sie, ob eventuell ein Energieverlust oder Überspannungen vorliegen. (Wenn Ihre Steckdosenleiste einen Schalter hat, schalten Sie diesen ein!)
- Wenn Sie das Problem immer noch nicht beheben konnten, ist eventuell die externe Stromversorgung defekt. Setzen Sie sich in diesem Fall mit dem Technischen Kundendienst in Verbindung, um Hilfe zu erhalten.

Das Signal ist ausgeschaltet

- Stellen Sie sicher, dass das Telefonkabel (RJ11) am ADSL Port Ihrer ADSL WLAN Basisstation und an der Telefonwanddose oder am Verteiler angeschlossen ist
- Prüfen Sie, ob Ihre Festnetzleitung korrekt funktioniert. Schließen Sie versuchsweise anstelle des Produktes ein Telefon an der Leitung an. Wenn Sie keinen Wählon erhalten, liegt das Problem an der Telefonleitung.

Das Signal @ ist immer ausgeschaltet

- Erkundigen Sie sich bei Ihrem Internet-Provider, ob Ihr Internet-Zugang freigeschaltet ist
- Lassen Sie sich Ihre Internet-Zugangsdaten von Ihrem Internet-Provider bestätigen

Die Signale 1 ... 4 erscheinen nicht. Im lokalen Netz kann kein Ping zur ADSL-WLAN-Basisstation ausgeführt werden.

- Wenn Sie eine Ethernetverbindung benutzen, stellen Sie sicher, dass Ihr TCP / IP korrekt installiert und auf Ihrem PC konfiguriert ist
- Stellen Sie sicher, dass das Ethernetkabel (RJ45) korrekt an Ihrer ADSL-WLAN-Basisstation angeschlossen ist
- Stellen Sie sicher, dass Sie das richtige Kabel für Ihre Ethernet-Geräte verwenden
- Stellen Sie sicher, dass die IP-Adresse korrekt konfiguriert ist. Für die meisten Anwendungen müssen Sie die DHCP-Funktion Ihrer ADSL WLAN-Basisstation benutzen, damit für alle im lokalen Netz-eingebundenen Hosts die IP-Adresse dynamisch zugewiesen wird. Falls Sie die IP-Adresse im lokalen Netz manuell konfigurieren, stellen Sie sicher, dass sowohl für die ADSL-WLAN-Basisstation als auch für alle eingebundenen LAN-Geräte dieselbe Netzwerkadresse und Subnetzmaske verwendet wird.

Das WLAN Netzwerk wird häufig unterbrochen

- Verringern Sie den Abstand zwischem Ihrem PC und der ADSL-WLAN-Basisstation, um die Signalstärke zu verbessern. Wenn das Signal immer noch schwach ist, ändern Sie den Winkel der Antenne. Es können auch Störungen durch Mikrowellenherde, eine drahtlose TV-Verbindung oder schnurlose Telefone hervorgerufen werden. Beheben Sie die Störungsquellen oder ändern Sie den Aufstellort der ADSL-WLAN-Basisstation.
- Sie können die drahtlosen Kanäle der ADSL-WLAN-Basisstation ändern. Siehe Webseite “Kanal und SSID/Channel and SSID”.

Copyright © 2007 Koninklijke Philips Electronics N.V.
All rights reserved.
Trademarks are the property of Koninklijke Philips Electronics N.V. or their respective owners.
Specifications are subject to change without notice.
Document order number : 3111 285 39951